ESET **MAIL SECURITY**

PER MICROSOFT EXCHANGE SERVER

Manuale di installazione e guida dell'utente

Microsoft® Windows® Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2

Fare clic qui per scaricare la versione più recente di questo documento

ESET MAIL SECURITY

Per ulteriori informazioni, visitare il sito Web www.eset.it.

Supporto tecnico: http://www.eset.it/supporto/assistenza-tecnica

REV. 21/10/2015

Contenuti

Contenuti

1. Introduzione

ESET Mail Security 6 for Microsoft Exchange Server è una soluzione integrata che offre uno strumento di protezione per le caselle di posta contro vari tipi di contenuti dannosi, compresi allegati di e-mail infettati da worm o trojan, documenti contenenti script pericolosi, schemi di phishing e spam. ESET Mail Security offre tre tipi di protezione: antivirus, antispam e regole definite dall'utente. ESET Mail Security filtra i contenuti dannosi a livello di server di posta prima che arrivino nella casella di posta del client del destinatario.

ESET Mail Security supporta Microsoft Exchange Server 2003 e versioni successive, oltre a Microsoft Exchange Server in un ambiente cluster. Nelle versioni più recenti (Microsoft Exchange Server 2003 e versioni successive), sono anche supportati ruoli specifici (casella di posta, hub e edge). ESET Remote Administrator consente di gestire ESET Mail Security da remoto in reti di grandi dimensioni.

Oltre a offrire protezione per Microsoft Exchange Server, ESET Mail Security include anche strumenti in grado di garantire la protezione del server stesso (protezione residente, protezione accesso Web e protezione client di posta).

1.1 Novità della versione 6

- Gestione quarantena e-mail: l'amministratore controlla gli oggetti in questa sezione di archiviazione e decide di eliminarli o rilasciarli. Questa funzione offre un sistema di gestione semplice delle e-mail messe in quarantena dall'agente di trasporto.
- Interfaccia Web della quarantena delle e-mail: alternativa basata sul Web alla gestione quarantena e-mail.
- Motore antispam: questo componente indispensabile è stato rinnovato ed è attualmente in corso di sviluppo.
- Controllo database su richiesta: lo scanner del database su richiesta utilizza l'API del complesso di servizi EWS (Exchange Web Services) per effettuare la connessione a Microsoft Exchange Server mediante HTTP/HTTPS.
- Regole**:** la voce del menu Regole consente agli amministratori di definire manualmente le condizioni di filtraggio delle e-mail e le azioni da eseguire con le e-mail filtrate. Le regole dell'ultima versione ESET Mail Security sono state ricreate da zero avvalendosi di un approccio diverso.
- ESET Cluster: questa soluzione, del tutto simile a ESET File Security 6 for Microsoft Windows Server, consente di collegare le workstation ai nodi allo scopo di offrire un maggior livello di automazione in termini di gestione, grazie alla sua capacità di distribuire un criterio di configurazione tra tutti i membri del cluster. La creazione degli stessi cluster può essere effettuata mediante l'utilizzo del nodo installato, che può quindi installare e iniziare tutti i nodi da remoto. I prodotti server ESET sono in grado di comunicare tra loro e scambiare dati quali configurazioni e notifiche, oltre a sincronizzare i dati necessari per il corretto funzionamento di un gruppo di istanze del prodotto. Tale funzione consente di eseguire la stessa configurazione del prodotto per tutti i membri di un cluster. I cluster di failover Windows e i cluster Network Load Balancing (NLB) sono supportati da ESET Mail Security. È inoltre possibile aggiungere manualmente i membri di ESET Cluster senza il bisogno di utilizzare un cluster Windows specifico. Gli ESET Cluster funzionano sia in ambienti di dominio sia in ambienti di gruppo di lavoro.
- Controllo archiviazione: controlla tutti i file condivisi su un server locale. Questa funzione facilita il controllo selettivo dei soli dati dell'utente archiviati sul server del file.
- Installazione basata sui componenti: l'utente ha facoltà di scegliere i componenti che desidera aggiungere o rimuovere.
- Esclusioni processi: esclude processi specifici dal controllo antivirus all'accesso. Il ruolo critico dei server dedicati (server dell'applicazione, server di archiviazione, ecc.) richiede backup periodici obbligatori allo scopo di garantire un recupero tempestivo da incidenti irreversibili di qualsiasi tipo. Per potenziare la velocità del backup, l'integrità del processo e la disponibilità del servizio, durante il backup vengono utilizzate alcune tecniche note per la loro capacità di entrare in conflitto con la protezione antivirus a livello dei file. Possono verificarsi problemi simili durante il tentativo di eseguire migrazioni live delle macchine virtuali. L'unico modo efficace per evitare queste due situazioni consiste nella disattivazione del software antivirus. Escludendo un processo specifico (ad esempio,

quelli della soluzione di backup), tutte le operazioni dei file attribuite al processo escluso vengono ignorate e considerate sicure, riducendo in tal modo l'interferenza con il processo di backup. Si consiglia di prestare la massima attenzione quando si creano le esclusioni, in quanto uno strumento di backup escluso può accedere a file infetti senza attivare un avviso. È questo il motivo per cui le autorizzazioni estese sono consentite esclusivamente nel modulo della protezione in tempo reale.

- ESET Log Collector: raccoglie automaticamente informazioni, come ad esempio quelle relative alla configurazione e a numerosi rapporti di ESET Mail Security. ESET Log Collector faciliterà la raccolta di informazioni diagnostiche necessarie per aiutare i tecnici ESET a risolvere rapidamente un problema.
- eShell (ESET Shell) - eShell 2.0 è ora disponibile in ESET Mail Security. eShell è un'interfaccia della riga di comando che offre agli utenti avanzati e agli amministratori opzioni più complete per la gestione dei prodotti server ESET.
- Hyper-V scan: è una nuova tecnologia che consente di controllare i dischi delle macchine virtuali (VM) su Microsoft Hyper-V Server senza la necessità di qualsiasi "Agente" sulla VM specifica.

1.2 Pagine della guida

Gentile cliente, siamo lieti di darle il benvenuto in ESET Mail Security. La presente guida è stata concepita allo scopo di aiutarla a sfruttare a pieno le funzionalità di ESET Mail Security.

Gli argomenti presentati nella guida sono suddivisi in vari capitoli e sottocapitoli. Per trovare le informazioni di cui ha bisogno, dovrà sfogliare la sezione **Contenuti** delle pagine della guida. In alternativa, sarà possibile utilizzare l'**Indice** per effettuare una ricerca in base alle parole chiave o utilizzare una **Ricerca** full-text.

Per ulteriori informazioni sulle finestre del programma, prema F1 sulla tastiera dopo aver aperto la finestra in questione. Verrà visualizzata la pagina della Guida relativa alla finestra correntemente visualizzata.

ESET Mail Security le consentirà di condurre ricerche tra gli argomenti della guida per parole chiave o attraverso la digitazione di parole o frasi all'interno del Manuale dell'utente. La differenza tra questi due metodi consiste nel fatto che una parola chiave può essere logicamente correlata a pagine della Guida che non contengono la specifica parola chiave nel testo. La ricerca di parole e frasi verrà invece eseguita nel contenuto di tutte le pagine e verranno visualizzate solo le pagine contenenti la parola o frase ricercata nel testo.

1.3 Metodi utilizzati

Per il controllo delle e-mail vengono utilizzati i tre seguenti metodi:

- Protezione database casella di posta: in precedenza nota come controllo casella di posta mediante VSAPI. Questo tipo di protezione è disponibile esclusivamente per Microsoft Exchange Server 2010, 2007 e 2003 che operano nel ruolo di Server della casella di posta (Microsoft Exchange 2010 e 2007) o di Server back-end (Microsoft Exchange 2003). Questo tipo di controllo viene eseguito sull'installazione di un singolo server con ruoli Exchange Server multipli su un computer (a condizione che sia presente il ruolo casella di posta o back-end).
- Protezione trasporto posta: precedentemente nota come filtraggio di messaggi sul livello del server SMTP. Questa protezione viene offerta dall'agente di trasporto ed è disponibile esclusivamente per Microsoft Exchange Server 2007 o versioni successive che operano nel ruolo di Server di trasporto Edge o di Server di trasporto Hub. Questo tipo di controllo viene eseguito sull'installazione di un singolo server con ruoli Exchange Server multipli su un computer (a condizione che sia presente uno dei ruoli del server indicati in precedenza).
- Controllo database su richiesta: consente all'utente di eseguire o pianificare un controllo del database delle caselle di posta di Exchange. Questa funzione è disponibile esclusivamente per Microsoft Exchange Server 2007 o versioni successive che operano nel ruolo di Server della casella di posta o di Trasporto Hub. Tale funzione si applica anche all'installazione di un singolo server con ruoli Exchange Server multipli su un computer (a condizione che sia presente uno dei ruoli del server indicati in precedenza). Consultare Ruoli di Exchange Server 2013 per maggiori informazioni sui ruoli in Exchange 2013.

1.3.1 Protezione database casella di posta

Il processo di controllo delle caselle di posta è attivato e gestito da Microsoft Exchange Server. Le e-mail nel database di archiviazione di Microsoft Exchange Server sono controllate continuamente. In base alla versione di Microsoft Exchange Server, la versione dell'interfaccia VSAPI e le impostazioni definite dagli utenti, è possibile attivare il processo di controllo nelle seguenti situazioni:

- Ad esempio, durante l'accesso dell'utente alle e-mail, in un client di posta (le e-mail vengono sempre controllate in base al database delle firme antivirali più recente)
- In background, in caso di scarso utilizzo di Microsoft Exchange Server
- In modo proattivo (in base all'algoritmo interno di Microsoft Exchange Server)

L'interfaccia VSAPI viene attualmente utilizzata per il controllo antivirus e la protezione basata su regole.

1.3.2 Protezione trasporto posta

Il filtraggio a livello del server SMTP viene protetto mediante un plug-in specializzato. In Microsoft Exchange Server 2000 e 2003, il plug-in in questione (*Event Sink*) viene registrato sul server SMTP come parte del complesso di servizi Internet Information Services (IIS). In Microsoft Exchange Server 2007/2010, il plug-in è registrato come agente di trasporto sul ruolo *Edge* o *Hub* di Microsoft Exchange Server.

Il filtraggio a livello del server SMTP da parte di un agente di trasporto offre protezione sotto forma di regole antivirus, antispam e definite dall'utente. Rispetto al filtraggio VSAPI, il filtraggio a livello del server SMTP viene eseguito prima dell'arrivo dell'e-mail controllata nella casella di posta di Microsoft Exchange Server.

1.3.3 Controllo database su richiesta

Poiché l'esecuzione di un controllo completo del database delle e-mail in ambienti di grandi dimensioni potrebbe causare un carico di sistema indesiderato, è possibile selezionare specifici database e caselle di posta da controllare. È possibile filtrare ulteriormente le destinazioni di controllo specificando l'indicatore data e ora dei messaggi da controllare per ridurre al minimo l'impatto sulle risorse di sistema del server.

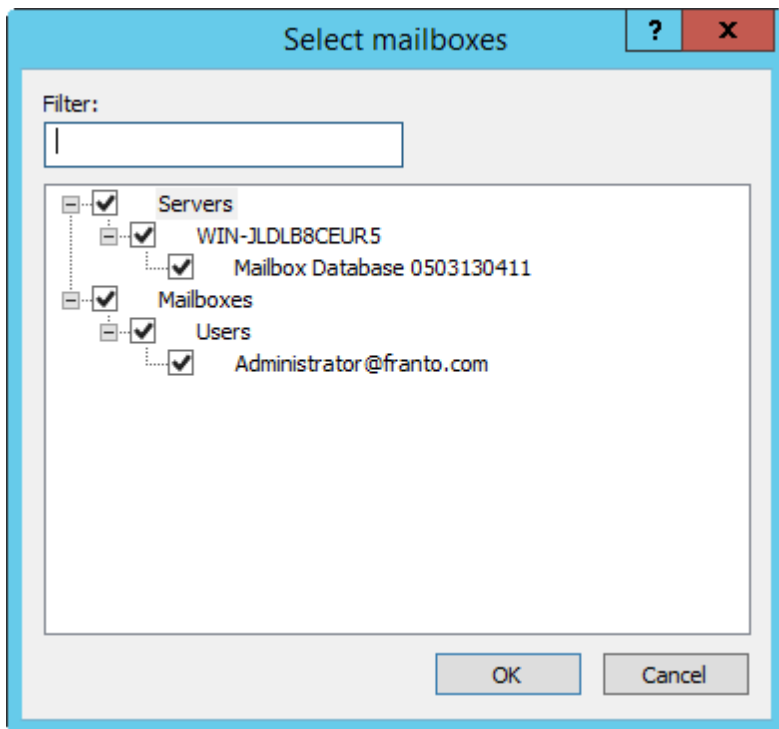
I seguenti tipi di oggetti vengono controllati sia nelle Cartelle pubbliche sia nelle Caselle di posta degli utenti:

- E-mail
- Pubblica
- Oggetti del calendario (riunioni/appuntamenti)
- Attività
- Contatti
- Diario

È possibile utilizzare l'elenco a discesa per scegliere i messaggi da controllare in base all'indicatore data e ora. Ad esempio, i messaggi modificati nell'ultima settimana. Se necessario, è inoltre possibile scegliere di controllare tutti i messaggi.

Selezionare la casella di controllo accanto a **Controlla corpi messaggi** per attivare o disattivare il controllo dei corpi dei messaggi.

Fare clic su **Modifica** per selezionare la cartella pubblica che verrà controllata.

Selezionare una o più caselle di controllo accanto ai database e alle caselle di posta del server che si desidera controllare. **Filtra** consente all'utente di trovare rapidamente i database e le caselle di posta, specialmente se nell'infrastruttura Exchange è presente un numero elevato di caselle di posta.

Fare clic su **Salva** per salvare le destinazioni e i parametri di controllo nel profilo del controllo su richiesta.

1.4 Tipi di protezione

Esistono tre tipi di protezione:

- Protezione antivirus
- Protezione antispam
- Applicazione di regole definite dall'utente

1.4.1 Protezione antivirus

La protezione antivirus rappresenta una delle funzioni di base di ESET Mail Security. La protezione antivirus difende il sistema da attacchi dannosi controllando file, e-mail e comunicazioni su Internet. In caso di rilevamento di una minaccia con codice dannoso, il modulo antivirus è in grado di eliminarla: prima bloccandola e poi pulendola, eliminandola o mettendola in Quarantena.

1.4.2 Protezione antispam

La protezione antispam integra varie tecnologie (RBL, DNSBL, lettore di impronte digitali, controllo reputazione, analisi contenuti, filtraggio Bayes, regole, whitelist/blacklist manuali, ecc.) per garantire un livello di rilevamento massimo delle minacce relative ai messaggi di posta elettronica. Il motore di controllo antispam produce un valore di probabilità sotto forma di percentuale (da 0 a 100) per ciascun messaggio di posta elettronica controllato.

ESET Mail Security utilizza anche il metodo greylist (disattivato per impostazione predefinita) del filtraggio antispam. Questo metodo si basa sulla specifica RFC 821, che stabilisce che, poiché SMTP è considerato un protocollo di trasporto inaffidabile, ogni agente di trasferimento messaggi (MTA) dovrebbe tentare ripetutamente di consegnare un'e-mail in seguito a un errore di consegna temporaneo. Molti messaggi spam vengono inviati una volta a un elenco in blocco di indirizzi di posta elettronica generato automaticamente. Il metodo greylist calcola un valore di controllo (hash) per l'indirizzo del mittente dell'envelope, l'indirizzo del destinatario dell'envelope e l'indirizzo IP dell'MTA che invia il messaggio. Se il server non trova il valore di controllo per la tripletta all'interno del proprio database, rifiuta l'accettazione del messaggio e rispedisce un codice di errore temporaneo (ad esempio,

451). Un server legittimo tenterà di inviare nuovamente il messaggio dopo un periodo di tempo variabile. Il valore di controllo della tripletta verrà archiviato nel database di connessioni verificate al secondo tentativo, consentendo l'invio di e-mail con caratteristiche rilevanti da questo punto in poi.

1.4.3 Applicazione di regole definite dall'utente

La protezione basata su regole è disponibile per i controlli sia con l'interfaccia VSAPI sia con l'agente di trasporto. È possibile utilizzare l'interfaccia utente di ESET Mail Security per creare regole individuali che si prestano anche a essere combinate. Se un ruolo utilizza condizioni multiple, queste verranno collegate mediante l'utilizzo dell'operatore logico E. Di conseguenza, la regola verrà eseguita solo se verranno soddisfatte tutte le condizioni. In caso di creazione di regole multiple, verrà utilizzato l'operatore logico O, che indica che il programma eseguirà la prima regola per la quale vengono soddisfatte le condizioni.

Nella sequenza di controllo, la prima tecnica utilizzata è il metodo greylist (se attivato). Le procedure successive eseguiranno sempre le seguenti tecniche: protezione basata su regole definite dall'utente, seguita da un controllo antivirus e, infine, controllo antispam.

1.5 Interfaccia utente

ESET Mail Security dispone di un'interfaccia utente (GUI) progettata per essere il più intuitiva possibile. L'interfaccia offre agli utenti un accesso semplice e rapido alle principali funzioni del programma.

Oltre all'interfaccia grafica utente principale (GUI), la **finestra di configurazione avanzata** è accessibile da qualsiasi schermata del programma premendo il tasto F5.

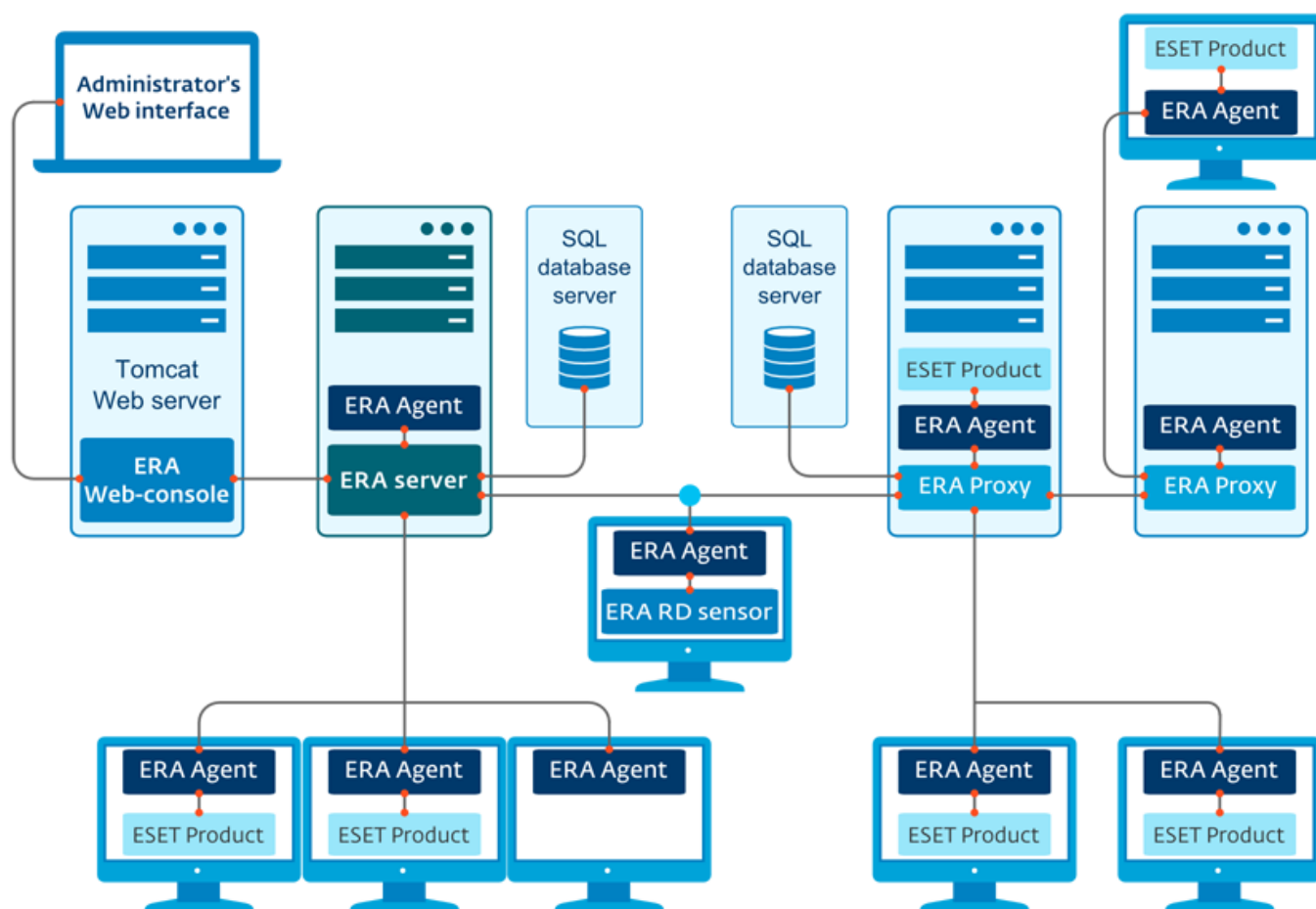
Dalla finestra Configurazione avanzata è possibile configurare le impostazioni e le opzioni preferite. Il menu sulla sinistra contiene le seguenti categorie: . Alcune categorie principali contengono sottocategorie. Facendo clic su un elemento (categoria o sottocategoria) nel menu sulla sinistra, le relative impostazioni vengono visualizzate sul riquadro di destra.

Per ulteriori informazioni sulla GUI, fare clic qui.

1.6 Gestione tramite ESET Remote Administrator

ESET Remote Administrator (ERA) è un'applicazione che consente all'utente di gestire i prodotti ESET in un ambiente di rete da una postazione centrale. Il sistema di gestione delle attività di ESET Remote Administrator offre l'installazione di soluzioni di protezione ESET su computer remoti e una risposta rapida ai nuovi problemi e alle nuove minacce. ESET Remote Administrator non garantisce protezione contro codice dannoso, ma si affida alla presenza della soluzione di protezione ESET su ciascun client.

Le soluzioni di protezione ESET supportano reti che includono vari tipi di piattaforme. Una rete può integrare, ad esempio, una combinazione degli attuali sistemi operativi Microsoft, Linux e OS X e dei sistemi operativi eseguiti sui dispositivi mobili (cellulari e tablet).

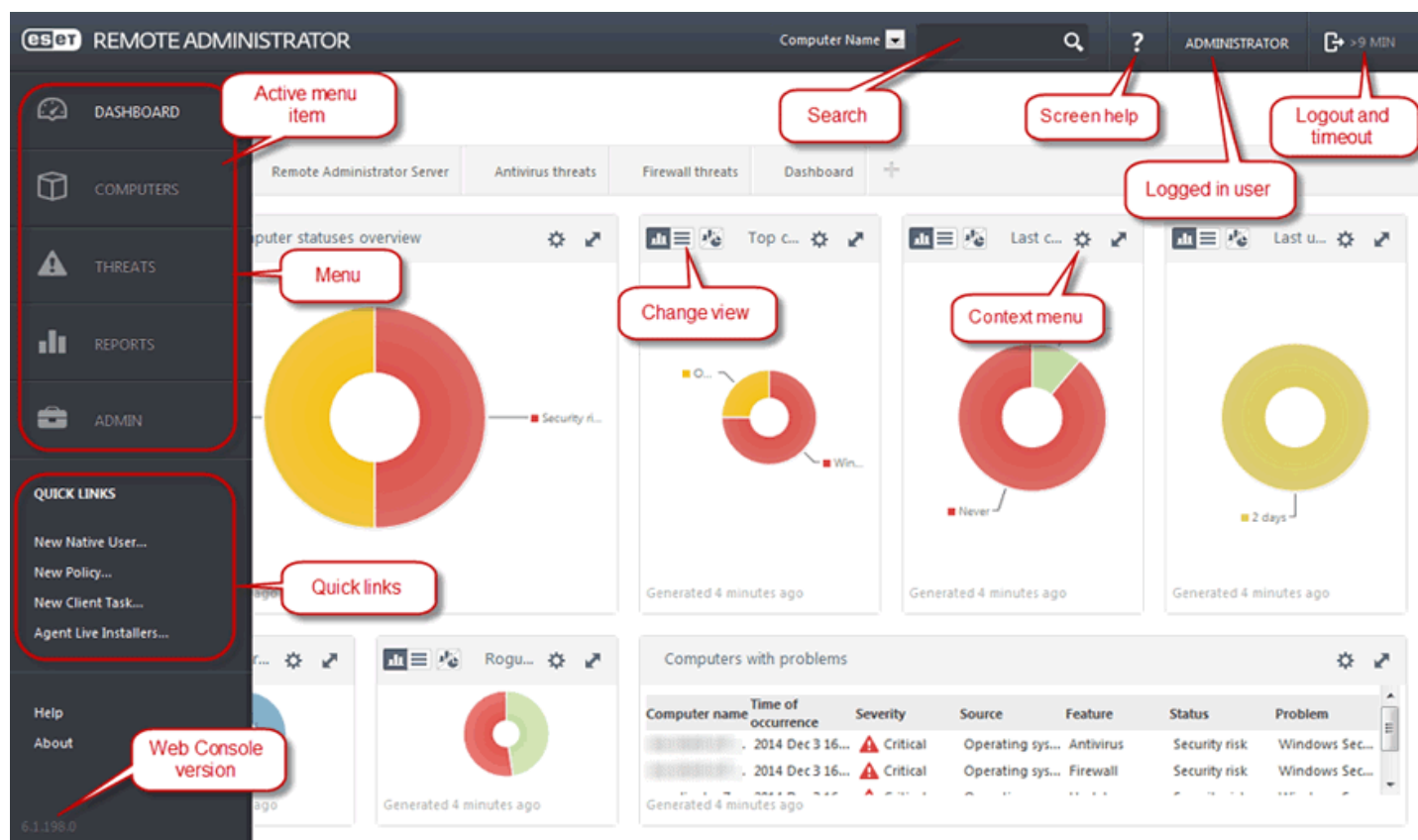
L'immagine sottostante illustra un esempio di architettura per una rete protetta mediante soluzioni di protezione ESET gestite da ERA:

NOTA: per ulteriori informazioni su ERA, consultare la <% Guida on-line di ESET_REMOTE_ADMINISTRATOR%>.

1.6.1 Server ERA

ESET Remote Administrator Server è un componente fondamentale di ESET Remote Administrator. È l'applicazione esecutiva che elabora tutti i dati ricevuti dai client che si connettono al server (attraverso l'Agente ERA). L'agente ERA facilita le comunicazioni tra il client e il server. I dati (rapporti del client, configurazione, replica dell'agente, ecc.) sono archiviati in un database. Per una corretta elaborazione dei dati, il server ERA richiede una connessione stabile al server di un database. Per ottenere prestazioni ottimali, si consiglia di installare il server ERA e il database su server separati. È necessario configurare la macchina sulla quale è installato il server ERA in modo da accettare tutte le connessioni dell'agente, del proxy o di RD Sensor, che vengono verificate mediante l'utilizzo dei certificati. Dopo aver installato il server ERA, è possibile aprire ERA Web Console che consente di effettuare la connessione al server ERA (come illustrato nel diagramma). Dalla Console Web, vengono eseguite tutte le operazioni del server ERA in caso di gestione della soluzione di protezione ESET all'interno della rete.

1.6.2 Console Web

ERA Web Console è un'interfaccia utente basata sul Web che presenta i dati provenienti dal Server ERA e consente all'utente di gestire le soluzioni di protezione ESET nell'ambiente in uso. È possibile accedere alla Console Web tramite un browser che consente di visualizzare una panoramica dello stato dei client sulla rete e di utilizzare da remoto soluzioni ESET su computer non gestiti. Nel caso in cui si decidesse di rendere il server Web accessibile da Internet, sarà possibile utilizzare ESET Remote Administrator da qualsiasi luogo e dispositivo in cui sia attiva una connessione a Internet.

Il dashboard della console Web è strutturato come segue:

Nella barra superiore della Console Web è disponibile lo strumento **Ricerca rapida**. Nel menu a discesa, selezionare **Nome computer**, **Indirizzo IPv4/IPv6** o **Nome minaccia**, digitare la stringa di ricerca nel campo di testo e fare clic sul simbolo della lente di ingrandimento oppure premere **Invio** per avviare la ricerca. L'utente verrà reindirizzato alla sezione Gruppi, dove potrà visualizzare i risultati delle ricerca: un client o un elenco di client. Tutti i client vengono gestiti tramite la Console Web. È possibile accedere alla Console Web mediante l'utilizzo di dispositivi e browser comuni.

NOTA: per ulteriori informazioni, consultare la <%Guida on-line di ESET_REMOTE_ADMINISTRATOR%>.

1.6.3 Agente

L'**Agente ERA** costituisce una parte essenziale del prodotto ESET Remote Administrator. Un prodotto ESET su una macchina client (ad esempio, ESET Endpoint security for Windows) comunica con il server ERA attraverso l'agente. Queste comunicazioni rendono possibile la gestione dei prodotti ESET su tutti i client remoti da una posizione centrale. L'agente raccoglie informazioni dal client e le invia al server. Se il server invia un'attività per il client, ciò significa che l'attività viene inviata all'agente che provvede poi a inviarla al client. Tutte le comunicazioni di rete avvengono tra l'agente e la parte superiore della rete ERA, ovvero il server e il proxy.

Per connettersi al server, l'agente ESET utilizza uno dei tre metodi seguenti:

1. L'agente del client è connesso direttamente al server.
2. L'agente del client è connesso mediante un proxy a sua volta connesso al server.
3. L'agente del client è connesso al server mediante proxy multipli.

L'agente ESET comunica con le soluzioni ESET installate su un client, raccoglie informazioni dai programmi installati su quel client e passa le informazioni di configurazione ricevute dal server al client.

NOTA: il proxy ESET possiede il proprio agente che gestisce tutte le attività di comunicazione tra i client, altri proxy e il server.

1.6.4 RD Sensor

L'**RD Sensor (Rogue Detection Sensor)** è uno strumento di ricerca per i computer presenti nella rete. L'applicazione, che fa parte di ESET Remote Administrator, è stata pensata allo scopo di rilevare le macchine presenti nella rete. È uno strumento che consente di aggiungere in modo pratico nuovi computer in ESET Remote Administrator senza che sia necessario eseguire l'operazione manualmente. Ogni computer trovato nella rete viene visualizzato nella console Web. Da qui, è possibile eseguire ulteriori azioni con singoli computer client.

RD Sensor è un ascoltatore passivo che rileva i computer presenti nella rete e invia le relative informazioni al server ERA. A questo punto, il server ERA valuta se i PC trovati nella rete sono sconosciuti o già gestiti.

1.6.5 Proxy

Il **Proxy ERA** è un altro componente di ESET Remote Administrator che consente di soddisfare due requisiti. In reti di medie dimensioni o aziendali caratterizzate dalla presenza di numerosi client (ad esempio, 10.000 client o più), è possibile utilizzare il proxy ERA per distribuire il carico tra molteplici proxy ERA, allo scopo di facilitare i compiti del Server ERA principale. L'altro vantaggio del proxy ERA consiste nella possibilità di utilizzarlo per connettersi a una filiale aziendale da remoto con un collegamento debole. Ciò significa che l'agente ERA su ciascun client non si connette al server ERA principale direttamente attraverso il proxy ERA che si trova sulla stessa rete locale della filiale. In questo modo libera il collegamento della filiale. Il proxy ERA accetta le connessioni da tutti gli agenti ERA locali, riunendo i relativi dati e caricandoli sul server ERA principale (o un altro proxy ERA). Tale operazione consente alla rete di adattare altri client senza compromettere le proprie prestazioni e la qualità delle query relative al database.

In base alla configurazione della rete in uso, il proxy ERA può connettersi a un altro proxy ERA per poi connettersi al server ERA principale.

Per un corretto funzionamento del proxy ERA, il computer host sul quale è stato installato il proxy ERA deve prevedere un agente ESET installato ed essere connesso al livello superiore (l'eventuale server ERA o un proxy ERA superiore) della rete in uso.

NOTA: per consultare un esempio dello scenario di distribuzione del proxy ERA, consultare la Guida on-line di ESET Remote Administrator.

2. Requisiti di sistema

Sistemi operativi supportati:

- Microsoft Windows Server 2003 (x86 e x64)
- Microsoft Windows Server 2003 R2 (x86 e x64)
- Microsoft Windows Server 2008 (x86 e x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

Versioni di Microsoft Exchange Server supportate:

- Microsoft Exchange Server 2003 SP1, SP2
- Microsoft Exchange Server 2007 SP1, SP2, SP3
- Microsoft Exchange Server 2010 SP1, SP2, SP3
- Microsoft Exchange Server 2013 CU2, CU3, CU4 (SP1), CU5, CU6, CU7, CU8
- Microsoft Exchange Server 2016

I requisiti hardware dipendono dalla versione del sistema operativo in uso. Per informazioni più dettagliate sui requisiti hardware, si consiglia di consultare la documentazione del prodotto Microsoft Windows Server.

3. Installazione

Dopo aver acquistato ESET Mail Security, è possibile scaricare il programma di installazione dal sito Web di ESET (www.eset.com) come pacchetto MSI.

Tenere presente che è necessario eseguire il programma di installazione con l'account Amministratore incorporato. Qualsiasi altro utente, pur essendo membro del gruppo Amministratori, non disporrà dei sufficienti diritti di accesso. Sarà pertanto necessario utilizzare l'account Amministratore incorporato poiché non sarà possibile completare correttamente l'installazione con qualsiasi altro account utente diverso da Amministratore.

Il programma di installazione può essere eseguito in due modi:

- È possibile eseguire l'accesso a livello locale utilizzando le credenziali dell'account Amministratore ed eseguire semplicemente il programma di installazione
- È possibile eseguire l'accesso come un altro utente ma è necessario aprire il prompt dei comandi con Esegui come... e immettere le credenziali dell'account Amministratore affinché il cmd sia eseguito come Amministratore, quindi digitare il comando per l'esecuzione del programma di installazione, ad esempio msiexec /i ma è necessario sostituire con il nome esatto del file del programma di installazione MSI scaricato.

Dopo aver avviato il programma di installazione e aver accettato l'Accordo di Licenza per l'Utente finale (ALUF), l'installazione guidata condurrà l'utente attraverso le fasi di configurazione. Se si sceglie di non accettare i termini dell'Accordo di licenza, la procedura guidata verrà interrotta.

Completa
Tipo di installazione consigliato che consente di installare tutte le funzionalità di ESET Mail Security. Dopo aver scelto questo tipo di installazione, sarà necessario specificare unicamente le cartelle dove installare il prodotto. Tuttavia, sarà possibile accettare anche le cartelle di installazione predefinite (scelta consigliata). Il programma di installazione installerà quindi automaticamente tutte le funzionalità del programma.

Personalizzato
Il tipo di installazione personalizzato consente di scegliere le funzionalità del programma di ESET Mail Security che saranno installate nel sistema. Verrà visualizzato un tipico elenco di funzionalità/componenti da selezionare per l'installazione.

Oltre all'installazione tramite la procedura guidata, è possibile installare ESET Mail Security in modalità automatica tramite la riga di comando. Questo tipo di installazione non richiede alcuna interazione rispetto alla procedura guidata descritta in precedenza. Risulta utile, ad esempio, per l'automazione o lo streamlining. Questo tipo di installazione viene anche detto senza interazione da parte dell'utente poiché non richiede alcun intervento da parte dell'utente.

Installazione silenziosa/senza l'intervento dell'utente
Installazione completa tramite la riga di comando: `msiexec /i <packagename> /qn /l*xv msi.log`

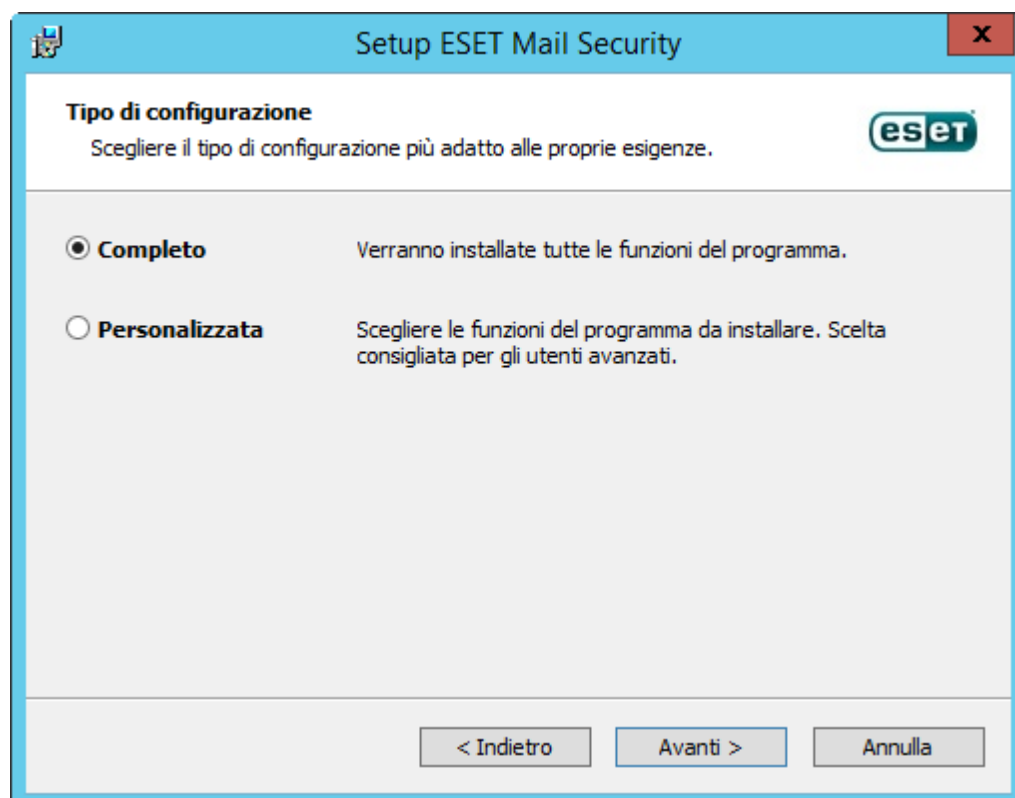
NOTA: è consigliabile installare ESET Mail Security su un sistema operativo appena installato e configurato, se possibile. Se è tuttavia necessario installarlo su un sistema esiste, è opportuno disinstallare la versione precedente di ESET Mail Security, riavviare il server e installare successivamente la nuova versione di ESET Mail Security.

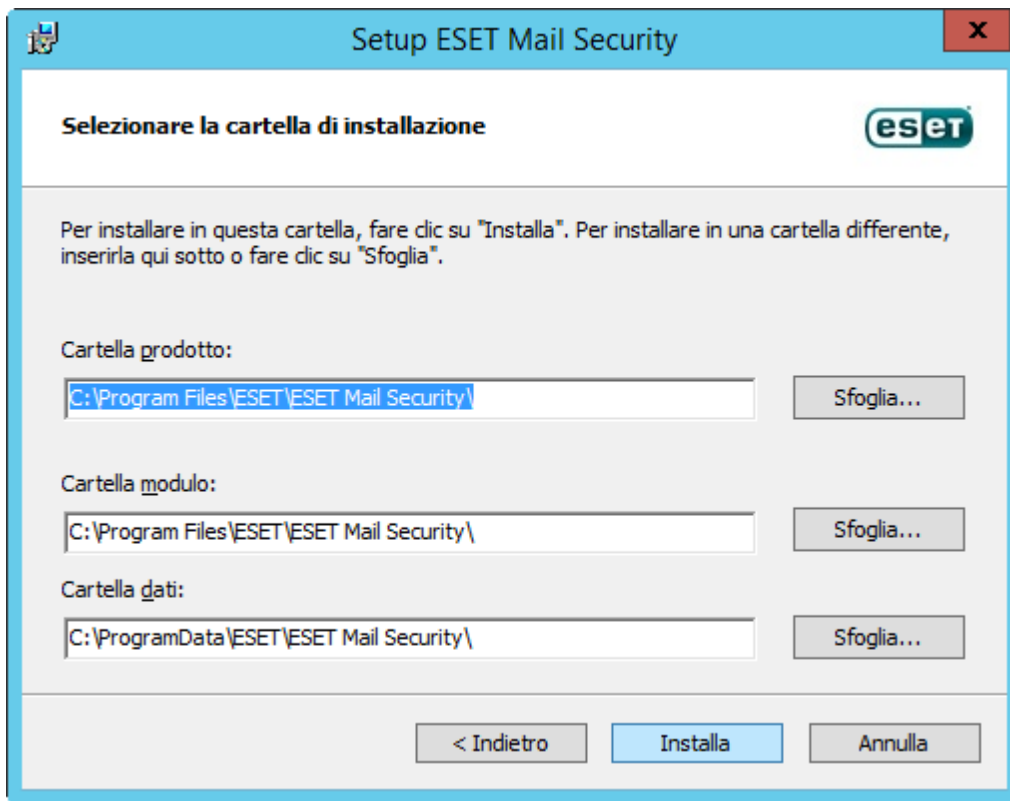
NOTA: se in precedenza è stato utilizzato un altro software antivirus di terze parti sul sistema, si consiglia di disinstallarlo completamente prima dell'installazione di ESET Mail Security. Per eseguire tale operazione, è possibile utilizzare ESET AV Remover che semplifica il processo di disinstallazione.

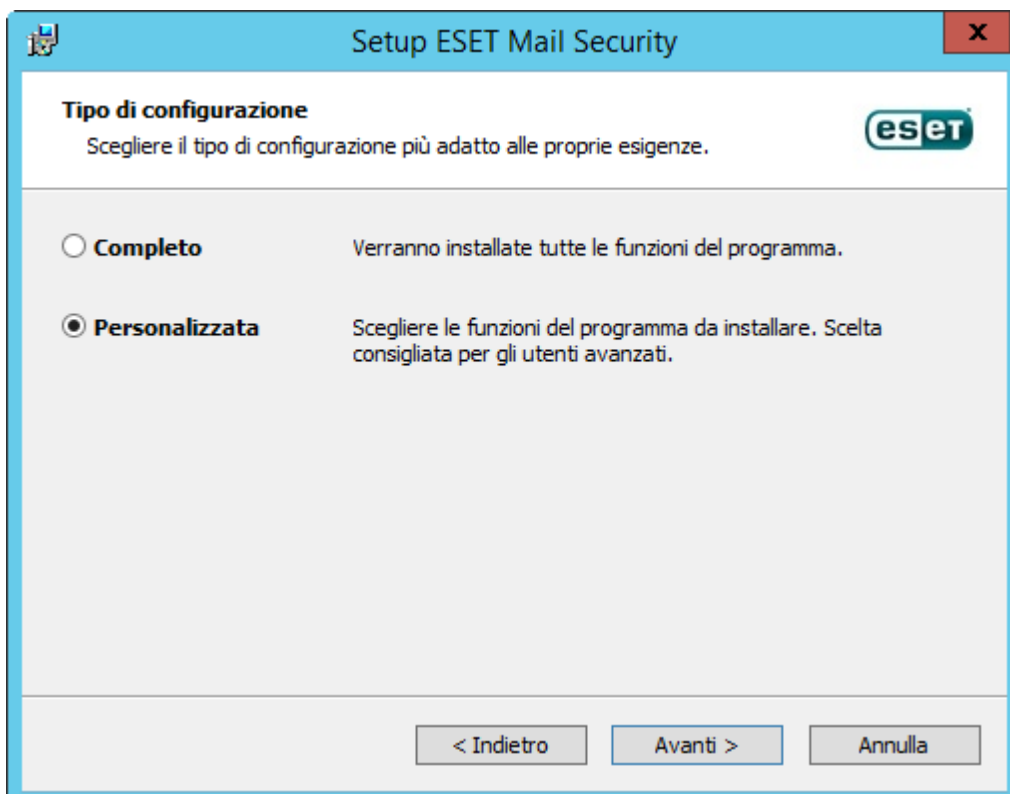
3.1 Passaggi di installazione di ESET Mail Security

Seguire i passaggi sottostanti per installare ESET Mail Security utilizzando la configurazione guidata:

Dopo aver accettato l'Accordo di licenza per l'utente finale (ALUF), è possibile scegliere tra i seguenti tipi di installazione:

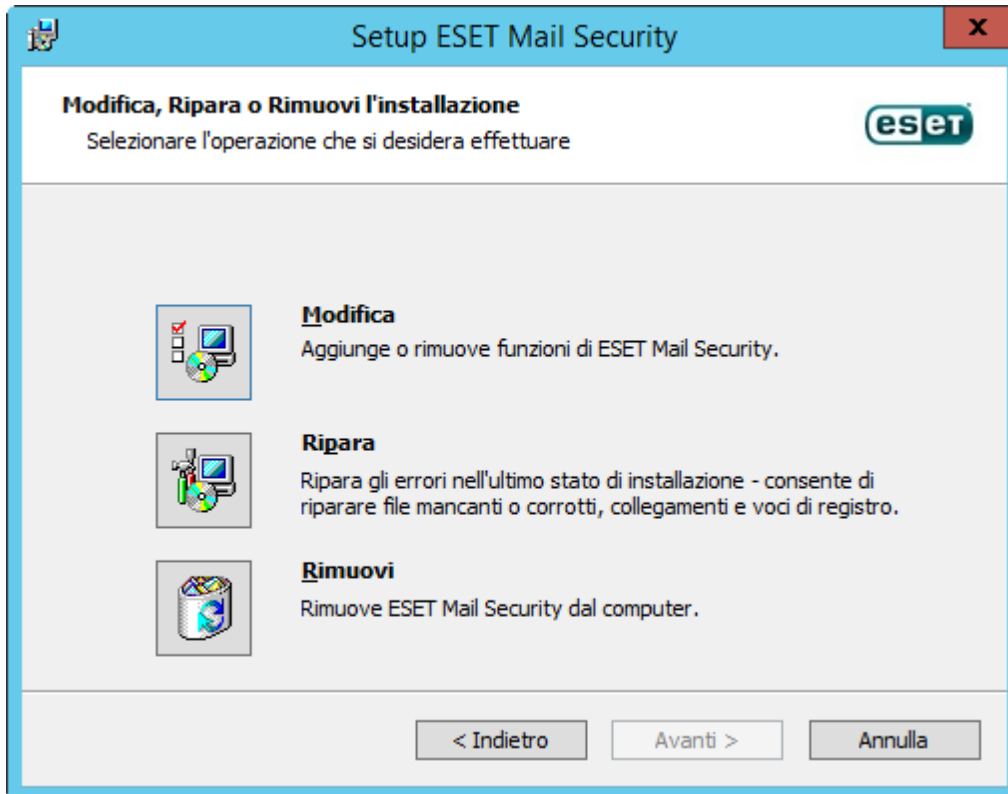
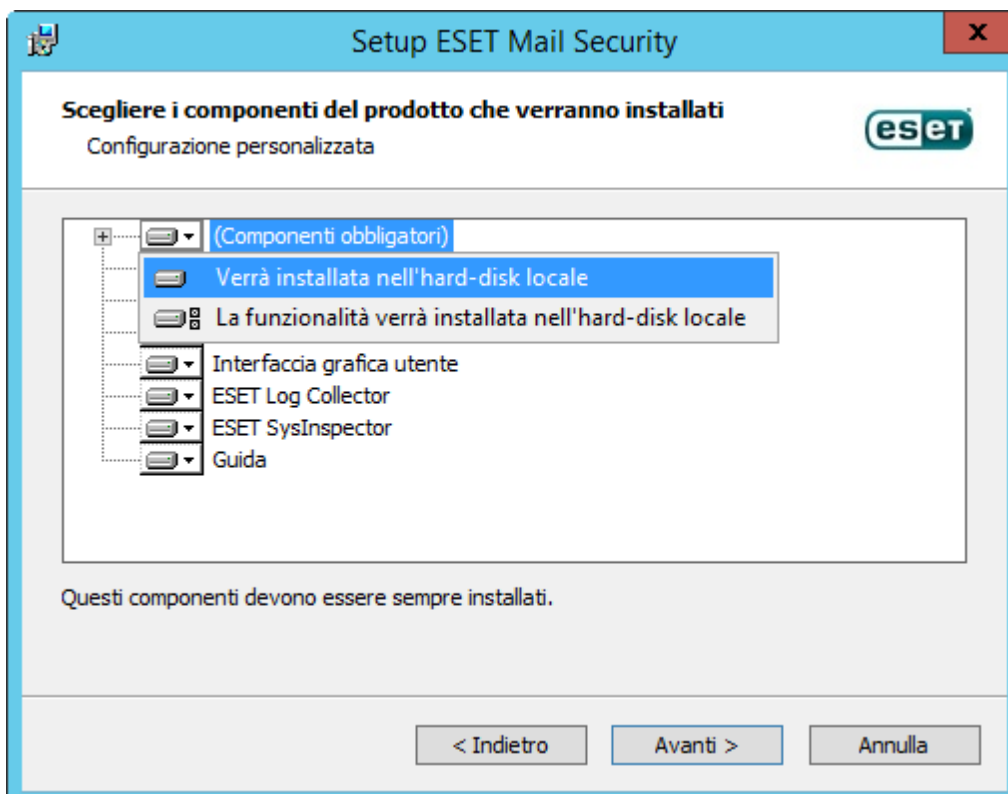
- **Completa**: installa tutte le funzioni di ESET Mail Security. Tipo di installazione consigliato.
- **Personalizzata**: selezionare le funzioni di ESET Mail Security che verranno installate sul sistema in uso.

Installazione completa:

nota anche come installazione completa di tutte le funzionalità. Tale operazione consentirà di installare tutti i componenti di ESET Mail Security. All'utente verrà richiesto di selezionare il percorso in cui verrà installato ESET Mail Security. Per impostazione predefinita, il programma viene installato nel percorso C:\Programmi\ESET\ESET Mail Security. Scegliere **Sfoglia** per selezionare un percorso diverso (scelta non consigliata).

Installazione personalizzata:

consente all'utente di scegliere le funzionalità che desidera installare. Risulta utile per personalizzare ESET Mail Security solo con i componenti necessari all'utente.

È possibile aggiungere o rimuovere i componenti inclusi nell'installazione. Per compiere tale operazione, eseguire il

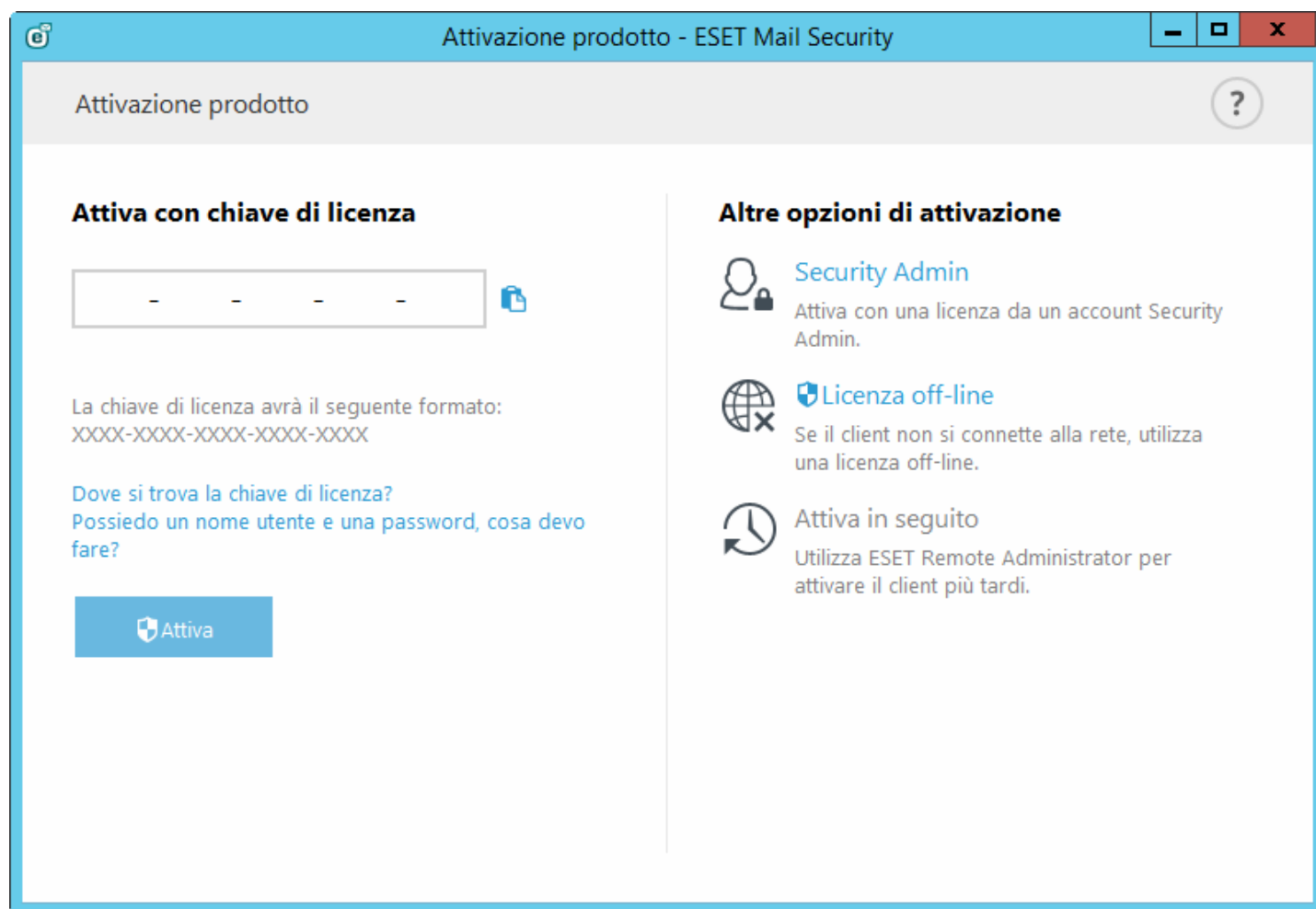
pacchetto di installazione .msi utilizzato durante l'installazione iniziale oppure accedere a **Programmi e funzioni** (accessibile dal Pannello di controllo di Windows), fare clic con il pulsante destro del mouse su ESET Mail Security e selezionare **Cambia**. Seguire i passaggi sottostanti per aggiungere o rimuovere i componenti.

Processo di modifica dei componenti (Aggiungi/Rimuovi), Ripara e Rimuovi:

Sono disponibili 3 opzioni. È possibile **Modificare** i componenti installati, **Riparare** l'installazione di ESET Mail Security o **Rimuoverlo** (disinstallarlo) completamente.

Se si sceglie **Modifica**, viene visualizzato un elenco dei componenti del programma disponibili. Scegliere i componenti che si desidera aggiungere o rimuovere. È possibile aggiungere/rimuovere contemporaneamente più di un componente. Fare clic sul componente e selezionare un'opzione dal menu a discesa:

Dopo aver selezionato un'opzione, fare clic su **Modifica** per attuare le modifiche.

ℹ **NOTA:** è possibile modificare i componenti installati in qualsiasi momento attraverso l'esecuzione del programma di installazione. Per la maggior parte dei componenti, non è necessario un riavvio del server per rendere effettive le modifiche. La GUI si riavvierà e sarà possibile visualizzare solo i componenti che si è deciso di installare. Per i componenti che richiedono un riavvio del server, Windows Installer chiederà all'utente di riavviare il sistema. A questo punto, i nuovi componenti diventeranno disponibili dopo che il server sarà ritornato on-line.

3.2 Attivazione prodotto

Al termine dell'installazione, all'utente verrà richiesto di attivare il prodotto.

Selezionare uno dei metodi disponibili per attivare ESET Mail Security. Per ulteriori informazioni, consultare Come fare per attivare ESET Mail Security.

Dopo aver attivato correttamente ESET Mail Security, la finestra principale del programma si aprirà e verrà visualizzato lo stato corrente nella pagina Monitoraggio.

Nella finestra principale del programma verranno inoltre visualizzate le notifiche relative ad altri elementi, come ad esempio gli aggiornamenti di sistema (aggiornamenti di Windows) o gli aggiornamenti del database delle firme antivirali. Se tutti gli elementi che richiedono attenzione vengono risolti, lo stato di monitoraggio diventerà verde e verrà visualizzato lo stato "**Massima protezione**".

3.3 Terminal Server

Se ESET Mail Security viene installato su un server Windows che funge da Terminal Server, l'utente potrebbe voler disattivare l'interfaccia utente di ESET Mail Security per impedire che venga avviata all'accesso di un utente. Per informazioni dettagliate su come disattivarla, consultare la sezione Disattiva l'interfaccia utente grafica su Terminal Server.

3.4 ESET AV Remover

Per rimuovere/disinstallare software antivirus di terze parti dal sistema in uso, si consiglia di utilizzare ESET AV Remover. Per compiere questa operazione, seguire i passaggi sottostanti:

1. Scaricare ESET AV Remover dallapagina di download delle utilità sul sito Web di ESET.
2. Fare clic su **Accetto, avvia la ricerca** per accettare l'Accordo di licenza per l'utente finale (ALUF) e avviare la ricerca nel sistema.
3. Fare clic su **Lancia programma di disinstallazione** per rimuovere il software antivirus installato.

Per consultare un elenco di software antivirus di terze parti che è possibile rimuovere utilizzando ESET AV Remover, consultare questo articolo della KB.

3.5 Aggiornamento a una versione più recente

Le nuove versioni di ESET Mail Securityvengono rilasciate per offrire miglioramenti o correggere errori che non è possibile risolvere mediante gli aggiornamenti automatici dei moduli del programma. È possibile effettuare l'aggiornamento dalle versione precedenti di ESET Mail Security (4.5 e precedenti) anche se l'aggiornamento è per architetture diverse. Esistono due modi per effettuare l'aggiornamento a una versione più recente:

- Manualmente scaricando e installando una versione più recente su quella esistente. Eseguire semplicemente il programma di installazione ed effettuare l'installazione normalmente: ESET Mail Security trasferirà automaticamente la configurazione esistente sebbene con qualche eccezione (consultare le note sotto).
- Da remoto, in un ambiente di rete, attraverso ESET Remote Administrator.

Importante: durante l'aggiornamento si verificano alcune eccezione e non tutte le impostazioni saranno conservate, specialmente quelle relative alle Regole. Ciò si verifica in quanto in ESET Mail Security 6 la funzionalità delle regole deve essere completamente creata di nuovo avvalendosi di un approccio diverso. Nelle versioni precedenti di ESET Mail Security le regole non sono compatibili con quelle di ESET Mail Security versione 6. Per semplificare la procedura, è consigliato configurare le Regole manualmente.

Attenendosi a un elenco di impostazioni conservate dalle versioni precedenti di ESET Mail Security:

- Configurazione generale di ESET Mail Security.
- Configurazione della protezione antispam:
  - Tutte le impostazioni sono identiche alle versioni precedenti e ogni impostazioni nuova utilizzerà i valori predefiniti.
  - Whitelist e blacklist.

NOTA: una volta effettuato l'aggiornamento di ESET Mail Security, è consigliato controllare tutte le impostazioni e assicurarsi che siano configurate correttamente e conformemente alle proprie esigenze.

3.6 Ruoli di Exchange Server: Edge vs Hub

Per impostazione predefinita, sui server di trasporto Edge e Hub le funzioni antispam sono disattivate. Questa rappresenta la configurazione consigliata in un'azienda che utilizza Exchange con un server di trasporto Edge. Si consiglia di configurare il server di trasporto Edge su cui è in esecuzione l'antispam ESET Mail Security in modo da filtrare i messaggi prima che vengano indirizzati verso l'azienda che utilizza Exchange.

Il ruolo Edge rappresenta la posizione preferita per il controllo antispam, grazie alla sua capacità di consentire a ESET Mail Security di rifiutare i messaggi di spam nelle prime fasi del processo senza creare un carico non necessario sui livelli della rete. Questa configurazione consente a ESET Mail Security di filtrare i messaggi in entrata sul server di trasporto Edge, che potranno in tal modo essere spostati in tutta sicurezza sul server di trasporto Hub senza il bisogno di ulteriori filtraggi.

Se l'azienda di appartenenza non utilizza un server di trasporto Edge ma solo un server di trasporto Hub, si consiglia di attivare le funzioni antispam sul server di trasporto Hub che riceve messaggi in entrata da Internet mediante SMTP.

3.7 Ruoli di Exchange Server 2013

L'architettura di Exchange Server 2013 è diversa dalle versioni precedenti di Microsoft Exchange. A partire dall'introduzione di Exchange 2013, CU4 (che corrisponde in realtà a SP1 per Exchange 2013) ha ripristinato il ruolo del server di trasporto Edge.

Qualora si decida di utilizzare ESET Mail Security per garantire la protezione di Microsoft Exchange 2013, assicurarsi di installarlo su un sistema in cui l'applicazione è in esecuzione con il ruolo di server della casella di posta o di trasporto Edge.

Qualora si decida di installare ESET Mail Security su Windows SBS (Small Business Server) o in caso di installazione di Microsoft Exchange 2013 con ruoli multipli su un server singolo, è prevista un'eccezione. In tal caso, tutti i ruoli di Exchange sono in esecuzione sullo stesso server. Di conseguenza, ESET Mail Security garantirà una protezione completa anche per i server di posta.

Qualora si decida di installare ESET Mail Security su un sistema sul quale è in esecuzione solo il ruolo del server Accesso client (server CAS dedicato), verranno disattivate le funzioni principali di ESET Mail Security, specialmente quelle relative al server di posta. In tal caso, saranno operativi esclusivamente la protezione file system in tempo reale e alcuni componenti appartenenti alla Protezione computer e, di conseguenza, i server di posta non saranno protetti. Per questo motivo, si sconsiglia di installare ESET Mail Security su un server con il ruolo Accesso client. Ciò non vale per Windows SBS (Small Business Server) e Microsoft Exchange con ruoli multipli sullo stesso computer, come illustrato in precedenza.

NOTA: a causa di restrizioni tecniche di Microsoft Exchange 2013, ESET Mail Security non supporta il ruolo del server Accesso client (CAS). Ciò non vale per Windows SBS o Microsoft Exchange 2013 installati su un server singolo con tutti i ruoli del server. In tal caso, è possibile eseguire ESET Mail Security con il ruolo CAS sul server, poiché il server della casella di posta e il server di trasporto Edge sono protetti.

3.8 Connettore e antispam POP3

Le versioni di Microsoft Windows Small Business Server (SBS) hanno un connettore nativo POP3 integrato che consente al server di recuperare i messaggi e-mail da server POP3 esterni. L'implementazione di questo connettore POP3 nativo di Microsoft varia in base alla versione di SBS.

ESET Mail Security supporta il connettore POP3 Microsoft SBS, purché sia configurato correttamente. I messaggi scaricati mediante il connettore POP3 Microsoft vengono controllati per verificare la presenta di spam. La protezione antispam per questi messaggi è possibile in quanto il connettore POP3 inoltra i messaggi e-mail provenienti da un account POP3 a Microsoft Exchange Server via SMTP.

ESET Mail Security è stato testato con i servizi di posta elettronica più utilizzati, come **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** e **gmx.de** sui sistemi SBS seguenti:

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Small Business Server 2008
- Microsoft Windows Small Business Server 2011

Importante: se si sta utilizzando il connettore POP3 integrato Microsoft SBS e tutti i messaggi e-mail vengono controllati per rilevare la presenza di spam, andare a Configurazione avanzata, quindi a **Server** > **Protezione trasporto posta** > Impostazioni avanzate, quindi, come impostazione per **Controlla anche messaggi ricevuti da connessioni interne o autenticate**, scegliere **Controlla tramite protezione antivirus e antispam** dall'elenco a discesa. In questo modo, è possibile assicurare che la protezione antispam sia attiva per le e-mail recuperate dagli account POP3.

È anche possibile utilizzare un connettore POP3 fornito da una terza parte, come P3SS, al posto del connettore POP3 integrato di Microsoft SBS POP3. ESET Mail Security è stato testato sui sistemi seguenti ed è stato utilizzato il connettore P3SS per recuperare i messaggi da **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** e **gmx.de**:

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Server 2008 con Exchange Server 2007
- Microsoft Windows Server 2008 R2 con Exchange Server 2010
- Microsoft Windows Server 2012 R2 con Exchange Server 2013

4. Guida introduttiva

In questo capitolo viene fornita una panoramica su ESET Mail Security, sui principali componenti del menu, sulle funzionalità e sulle impostazioni di base.

4.1 L'interfaccia utente

La finestra principale di ESET Mail Security è suddivisa in due sezioni principali. La finestra principale sulla destra contiene informazioni corrispondenti all'opzione selezionata dal menu principale sulla sinistra.

Le varie sezioni del menu principale sono descritte di seguito:

Monitoraggio: offre informazioni sullo stato di protezione di ESET Mail Security, sulla validità della licenza, sull'ultimo aggiornamento del database delle firme antivirali, sulle statistiche di base e sui dati del sistema.

File di rapporto: consente di accedere ai file di rapporto contenenti informazioni su tutti gli eventi di programma importanti che si sono verificati. Questi file offrono una panoramica delle minacce rilevate nonché di altri eventi correlati alla sicurezza.

Controllo: consente all'utente di configurare e avviare un controllo archiviazione, un controllo intelligente, un controllo personalizzato o un controllo di supporti rimovibili. È inoltre possibile ripetere l'ultimo controllo eseguito.

Aggiornamento: consente di visualizzare informazioni sul database delle firme antivirali e invia una notifica all'utente in caso di disponibilità di un aggiornamento. Da questa sezione è inoltre possibile eseguire l'attivazione del prodotto.

Configurazione: qui è possibile regolare le impostazioni di protezione del server e del computer.

Strumenti: offre informazioni aggiuntive sul sistema e sulla protezione oltre agli strumenti che consentono all'utente di potenziare il livello di gestione dei sistemi di sicurezza. La sezione Strumenti contiene i seguenti elementi: Processi in esecuzione, Attività di verifica, ESET Log Collector, Statistiche di protezione, Cluster, ESET Shell, ESET SysInspector, ESET SysRescue Live per la creazione di un CD o USB di ripristino e Pianificazione attività. È inoltre possibile Inviare un campione per l'analisi e controllare la cartella Quarantena.

Guida e supporto tecnico: consente di accedere alle pagine della Guida, alla Knowledge Base ESET e ad altri strumenti di assistenza. Sono inoltre disponibili collegamenti per l'invio di una richiesta di assistenza al Supporto tecnico e informazioni relative all'attivazione del prodotto.

Nella schermata **Stato protezione** sono disponibili informazioni sul livello di protezione corrente del computer. Lo stato **Massima protezione** (di colore verde) indica che è garantito il livello massimo di protezione.

La finestra Stato consente inoltre di visualizzare collegamenti rapidi alle funzioni utilizzate più frequentemente in ESET Mail Security e alle informazioni relative all'ultimo aggiornamento.

Cosa fare se il programma non funziona correttamente?

Ai moduli che funzionano correttamente viene assegnato un segno di spunta di colore verde. Ai moduli che non funzionano correttamente viene assegnato un punto esclamativo di colore rosso o un'icona di notifica di colore arancione. Nella parte superiore della finestra verranno visualizzate ulteriori informazioni sul modulo. Verrà inoltre visualizzata una soluzione consigliata per la riparazione del modulo. Per modificare lo stato di un singolo modulo, fare clic su **Configurazione** nel menu principale, quindi sul modulo desiderato.

L'icona di colore rosso indica che sono presenti problemi critici, ovvero che non è garantito il livello massimo di protezione del computer. Questo stato viene visualizzato nei casi che seguono:

- **Protezione antivirus e antispyware disattivata**: è possibile riattivare la protezione antivirus e antispyware facendo clic su **Attiva protezione in tempo reale** nel riquadro **Stato protezione** o su **Attiva protezione antivirus e antispyware** nel riquadro **Configurazione** della finestra principale del programma.
- Si sta utilizzando un database delle firme antivirali obsoleto.
- Il prodotto non è attivato.
- **Licenza scaduta**: questa condizione è indicata dalla presenza di un'icona rossa dello stato di protezione. Allo scadere della licenza, non sarà possibile aggiornare il programma. Si consiglia di seguire le istruzioni indicate nella finestra di avviso per rinnovare la licenza.

L'icona di colore arancione indica che il prodotto ESET richiede attenzione per un problema non critico. Le cause possibili sono:

- **La protezione accesso Web è disattivata**: è possibile riattivare la protezione accesso Web facendo clic sulla notifica di protezione, quindi su **Attiva protezione accesso Web**.

- **La licenza scadrà a breve**: questa condizione è indicata dalla presenza dell'icona dello stato di protezione con un punto esclamativo. Allo scadere della licenza, non sarà possibile aggiornare il programma e l'icona dello stato di

protezione diventerà rossa.

Qualora non si riuscisse a risolvere un problema ricorrendo alle soluzioni consigliate, fare clic su **Guida e supporto tecnico** per accedere ai file della guida oppure effettuare una ricerca nella Knowledge Base ESET. Nel caso in cui sia necessaria ulteriore assistenza, è possibile inviare una richiesta al Supporto tecnico ESET. Il Supporto tecnico ESET risponderà rapidamente alle domande degli utenti e li aiuterà a trovare una soluzione ai loro problemi.

Per visualizzare lo **Stato protezione**, fare clic sulla prima opzione nel menu principale. Nella finestra principale verrà visualizzato un riepilogo sullo stato di funzionamento di ESET Mail Security. Verrà inoltre visualizzato un sottomenu con due elementi: **Attività di verifica** e **Statistiche**. Selezionare una delle due opzioni per visualizzare informazioni più dettagliate sul sistema.

Se ESET Mail Security viene eseguito con le funzionalità complete, **l'icona dello Stato protezione** appare in verde. Se è richiesta l'attenzione dell'utente, l'icona sarà di colore arancione o rosso.

Fare clic su **Attività di verifica** per visualizzare un grafico in tempo reale dell'attività del file system (asse orizzontale). Sull'asse verticale viene mostrata la quantità di dati letti (riga blu) e dati scritti (riga rossa).

Il sottomenu **Statistiche** consente di visualizzare il numero di oggetti infettati, puliti e non infetti di un modulo specifico. Nell'elenco a discesa sono disponibili diversi moduli tra i quali poter scegliere.

4.2 File di rapporto

I file di rapporto contengono informazioni relative agli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate. I rapporti sono essenziali per l'analisi del sistema, il rilevamento delle minacce e la risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento da parte dell'utente. Le informazioni vengono registrate in base alle impostazioni del livello di dettaglio di rapporto. È possibile visualizzare i messaggi di testo e i rapporti direttamente dall'ambiente di ESET Mail Security o esportarli per poterli visualizzare altrove.

È possibile accedere ai file di rapporto dalla finestra principale del programma facendo clic su **File di rapporto**. Selezionare il tipo di rapporto desiderato nel menu a discesa. Sono disponibili i rapporti seguenti:

- **Minacce rilevate**: nel rapporto delle minacce sono contenute informazioni dettagliate sulle infiltrazioni rilevate dai moduli ESET Mail Security. Queste includono l'ora del rilevamento, il nome dell'infiltrazione, la posizione, l'azione eseguita e il nome dell'utente registrato nel momento in cui è stata rilevata l'infiltrazione. Fare doppio clic su una voce qualsiasi del rapporto per visualizzarne il contenuto dettagliato in una finestra separata.
- **Eventi**: tutte le azioni importanti eseguite da ESET Mail Security vengono registrate nel rapporto eventi. Il rapporto eventi contiene informazioni sugli eventi e gli errori che si sono verificati nel programma. È stato progettato per aiutare gli amministratori di sistema e gli utenti a risolvere i problemi. Spesso le informazioni visualizzate in questo rapporto consentono di trovare la soluzione a un problema che si verifica nel programma.
- **Controllo del computer**: tutti i risultati del controllo possono essere visualizzati in questa finestra. Ogni riga corrisponde a un singolo controllo del computer. Fare doppio clic su una voce qualsiasi per visualizzare i dettagli del rispettivo controllo.
- **HIPS**: contiene i record di regole specifiche che sono stati contrassegnati per la registrazione. Nel protocollo è possibile visualizzare l'applicazione che ha invocato l'operazione, il risultato (ovvero se la regola era consentita o vietata) e il nome della regola creata.
- **Siti Web filtrati**: elenco di siti Web bloccati dalla Protezione accesso Web. In questi rapporti è possibile visualizzare l'ora, l'URL, l'utente e l'applicazione che hanno aperto una connessione a un sito Web specifico.
- **Controllo dispositivi**: contiene record relativi ai supporti rimovibili o ai dispositivi collegati al computer. Nel file di rapporto saranno registrati solo i dispositivi con una regola di controllo dispositivi. Se la regola non corrisponde a un dispositivo collegato, non verrà creata alcuna voce di rapporto relativa a tale evento. Qui è possibile visualizzare anche dettagli relativi al tipo di dispositivo, al numero di serie, al nome del fornitore e alle dimensioni del supporto (ove disponibili).
- **Controllo database**: contiene la versione del database delle firme antivirali, la data, la posizione controllata, il numero di oggetti controllati, il numero di minacce trovate, il numero di attivazioni della regola e l'ora di completamento.
- **Protezione server di posta** Tutti i messaggi categorizzati da ESET Mail Security come o potenzialmente come spam vengono registrati qui. Questi registri sono pertinenti ai tipi di protezione seguenti: Antispam, Regole e Antivirus.
- **Greylist**: tutti i messaggi che sono stati valutati mediante l'utilizzo del metodo greylist sono registrati qui.

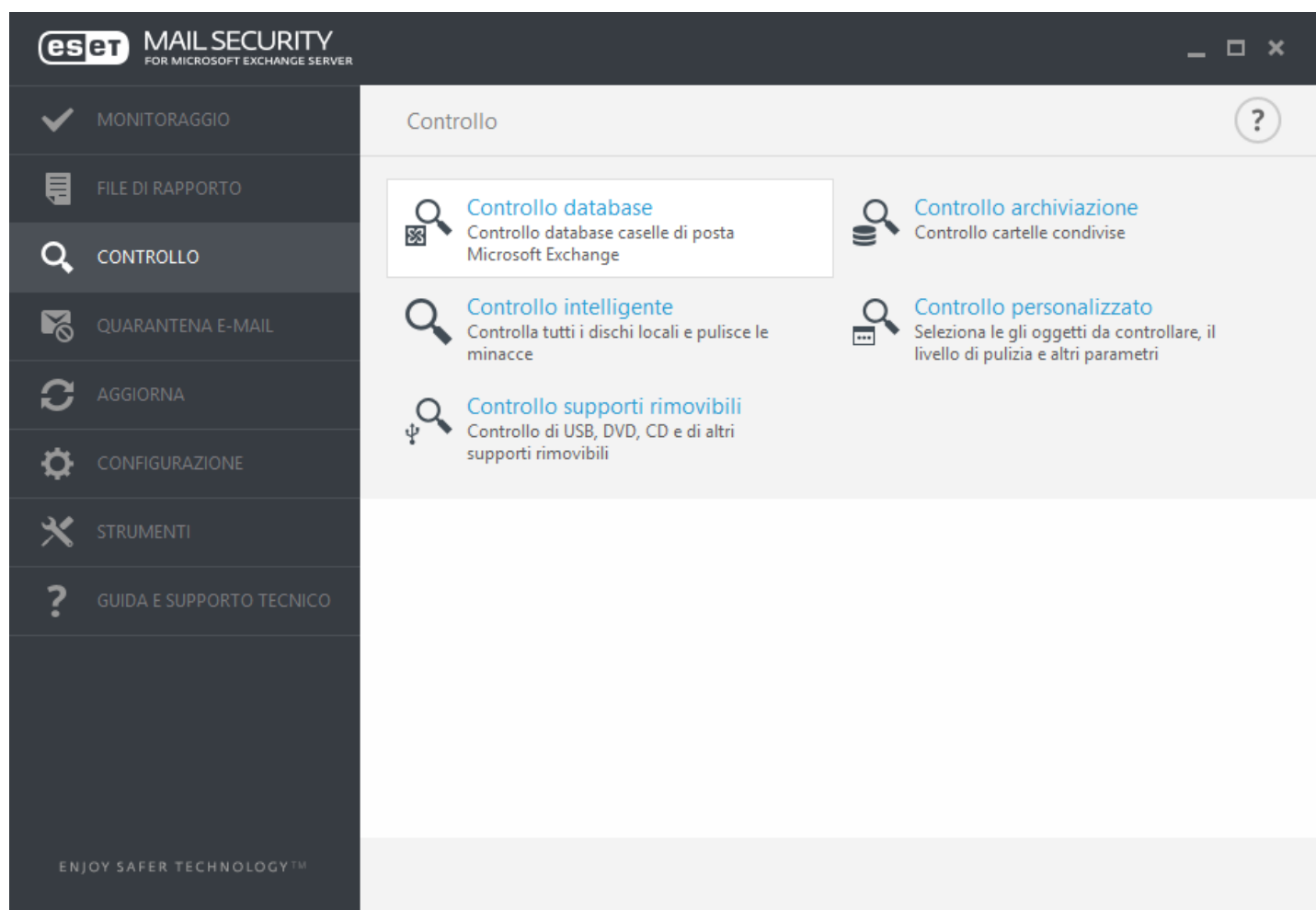
In ciascuna sezione, le informazioni visualizzate possono essere copiate negli Appunti (tasto di scelta rapida Ctrl + C), selezionando la voce desiderata e facendo clic su **Copia**. Per selezionare più voci, utilizzare i tasti CTRL e MAIUSC.

Fare clic sull'icona del pulsante **Filtraggio** per aprire la finestra **Filtraggio rapporti** in cui è possibile definire i criteri di filtraggio.

Fare clic con il pulsante destro del mouse su un record specifico per far comparire il menu contestuale. Nel menu contestuale sono disponibili le seguenti opzioni:

- **Mostra**: consente di visualizzare informazioni più dettagliate relative al rapporto selezionato in una nuova finestra (funzione uguale all'esecuzione di un doppio clic).
- **Filtra gli stessi record**: questa opzione attiva il filtraggio dei rapporti e consente di visualizzare esclusivamente i record dello stesso tipo di quello selezionato.
- **Filtra...**: dopo aver selezionato questa opzione, la finestra Filtraggio rapporti consentirà all'utente di definire i criteri di filtraggio per voci specifiche dei rapporti.
- **Attiva filtro**: attiva le impostazioni del filtro. Durante il primo filtraggio dei rapporti, è necessario definirne i criteri. Una volta impostati, i filtri rimarranno invariati fino alla successiva modifica da parte dell'utente.
- **Copia**: copia le informazioni dai record selezionati/evidenziati negli Appunti.
- **Copia tutto**: copia le informazioni di tutti i record nella finestra.
- **Elimina**: elimina i record selezionati/evidenziati. Per poter eseguire questa operazione è necessario disporre dei privilegi amministrativi.
- **Elimina tutto**: elimina tutti i record nella finestra. Per poter eseguire questa operazione è necessario disporre dei privilegi amministrativi.
- **Esporta...**: esporta le informazioni dai record selezionati/evidenziati in un file XML.
- **Esporta tutto...** : esporta tutte le informazioni presenti nella finestra in un file XML.
- **Trova...**: apre la finestra Trova nel rapporto e consente all'utente di definire i criteri di ricerca. Lavora sui contenuti che sono già stati filtrati fungendo da strumento aggiuntivo per la riduzione dei risultati.
- **Trova successiva**: trova l'occorrenza successiva di una ricerca precedentemente definita (vedere sopra).
- **Trova precedente**: trova l'occorrenza precedente di una ricerca precedentemente definita (vedere sopra).
- **Scorri registro**: lasciare attivata questa opzione per scorrere automaticamente i rapporti meno recenti e visualizzare i rapporti attivi nella finestra **File di rapporto**.

4.3 Controllo

Lo scanner su richiesta rappresenta un componente importante di ESET Mail Security. Viene utilizzato per eseguire il controllo di file e di cartelle sul computer in uso. Dal punto di vista della protezione, è essenziale che i controlli del computer non vengano eseguiti solo quando si sospetta un'infezione, ma periodicamente, nell'ambito delle normali misure di protezione. Si consiglia di eseguire controlli approfonditi periodici (ad esempio, una volta al mese) del sistema allo scopo di rilevare virus non trovati dalla Protezione file system in tempo reale. Ciò può verificarsi se la protezione file system in tempo reale era disattivata in quel momento, il database antivirus era obsoleto o il file non è stato rilevato come virus nel momento in cui è stato salvato sul disco.

Sono disponibili due tipologie di **Controllo del computer**. **Controllo intelligente**, che consente di eseguire rapidamente il controllo del sistema senza che sia necessario configurare ulteriori parametri. **Controllo personalizzato**, che consente all'utente di selezionare un qualsiasi profilo di controllo predefinito e di definire specifiche destinazioni di controllo.

Per ulteriori informazioni sull'avanzamento del controllo, consultare il capitolo Avanzamento controllo.

Controllo archiviazione

Consente di eseguire il controllo di tutte le cartelle condivise sul server locale. Se il **Controllo archiviazione** non è disponibile, ciò significa che non sono presenti cartelle condivise sul server.

Controllo Hyper-V

Questa opzione è visibile nel menu solo se Hyper-V Manager è installato sul server in cui è in esecuzione ESET Mail Security. Hyper-V scan consente il controllo dei dischi delle macchine virtuali (VM) su Microsoft Hyper-V Server senza che sia necessario installare qualsiasi "Agente" sulla VM specifica. Per ulteriori informazioni, vedere Hyper-V scan.

Controllo intelligente

La funzione Controllo intelligente consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il vantaggio del controllo intelligente consiste nella facilità di utilizzo e nel fatto che non è richiesta una configurazione di controllo dettagliata. Il Controllo intelligente consente di effettuare un controllo di tutti i file presenti nelle unità locali, nonché una pulizia o un'eliminazione automatica delle infiltrazioni rilevate. Il livello di pulizia viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di pulizia, consultare il paragrafo Pulizia.

Controllo personalizzato

Il controllo personalizzato è una soluzione ottimale se si desidera specificare parametri di controllo quali destinazioni di controllo e metodi di controllo. Il vantaggio del Controllo personalizzato consiste nella possibilità di configurare i parametri in dettaglio. È possibile salvare le configurazioni come profili di controllo definiti dagli utenti che risultano particolarmente utili se il controllo viene eseguito più volte utilizzando gli stessi parametri.

Per scegliere le destinazioni di controllo, selezionare **Controllo computer** > **Controllo personalizzato** e scegliere un'opzione dal menu a discesa **Destinazioni di controllo** oppure specifiche destinazioni di controllo dalla struttura ad albero. Una destinazione di controllo può anche essere specificata immettendo il percorso della cartella o del/i file che si desidera includere. Se si desidera effettuare solo un controllo del sistema senza azioni di pulizia aggiuntive, selezionare **Controlla senza pulire**. Durante l'esecuzione di un controllo, è possibile scegliere uno dei tre livelli di pulizia facendo clic su **Configurazione** > **Parametri ThreatSense** >**Pulizia**.

L'esecuzione di controlli del computer attraverso il controllo personalizzato è consigliata solo per utenti avanzati con precedenti esperienze di utilizzo di programmi antivirus.

Controllo supporti rimovibili

Simile al Controllo intelligente: consente di lanciare velocemente un controllo dei supporti rimovibili (come ad esempio CD/DVD/USB) collegati al computer. Questa opzione può rivelarsi utile in caso di connessione di una memoria USB a un computer e nel caso in cui si desideri ricercare malware e altre potenziali minacce.

Questo tipo di controllo può anche essere avviato facendo clic su **Controllo personalizzato**, quindi selezionando **Supporti rimovibili** dal menu a discesa **Destinazioni di controllo** e facendo clic su **Controllo**.

Ripeti ultimo controllo

Esegue l'ultimo controllo, indipendentemente da quale sia stato (archiviazione, intelligente, personalizzato e così via), con le stesse identiche impostazioni.

i **NOTA:** è consigliabile eseguire un controllo del computer almeno una volta al mese. Il controllo può essere configurato come attività pianificata da **Strumenti** > **Pianificazione attività**.

4.3.1 Controllo Hyper-V

Il controllo antivirus Hyper-V consente il controllo dei dischi di un Microsoft Hyper-V Server, ovvero, di una macchina virtuale (VM) senza che sia necessario aver installato un qualsiasi Agente sulla VM specifica. L'antivirus è installato utilizzando i privilegi di Amministratore del server Hyper-V.

Il controllo Hyper-V è derivato dal modulo Controllo computer su richiesta, mentre alcune funzionalità non sono state implementate (controllo del settore di avvio, sarà implementato più avanti, controllo della memoria operativa).

Sistemi operativi supportati

- Windows Server 2008 R2: le macchine virtuali che eseguono questo sistema operativo possono essere sottoposte a controllo solo se non sono in linea
- Windows Server 2012
- Windows Server 2012 R2

Requisiti hardware

Il server non dovrebbe presentare problemi di prestazioni nell'esecuzione delle macchine virtuali. Il controllo utilizza principalmente solo le risorse della CPU.
Nel caso del controllo online, è necessario spazio libero su disco della VM. Lo spazio su disco (disponibile per l'uso) deve essere almeno il doppio dello spazio utilizzato dagli snapshot e dai dischi virtuali.

La macchina virtuale da controllare non è in linea (spenta)

Grazie agli Strumenti di gestione Hyper-V e al supporto dei dischi virtuali, sono stati rilevati i dischi del sistema operativo della macchina virtuale ed è stata eseguita la connessione ad essi. In questo modo, si dispone dello stesso accesso ai contenuti dei dischi come se si accedesse ai file di un hard disk generale.

La macchina virtuale da controllare è in linea (in esecuzione, sospesa, salvata)

Grazie agli Strumenti di gestione Hyper-V e al supporto del dischi virtuali, sono stati rilevati i dischi del sistema operativo della macchina virtuale ed è stata eseguita la connessione ad essi. Al momento non è disponibile una connessione generica ai dischi. Pertanto, è stato creato uno snapshot della macchina virtuale e tramite di esso è stata eseguita la connessione ai dischi in modalità di sola lettura. Al termine del controllo, lo snapshot viene eliminato.
La creazione di uno snapshot rappresenta un'operazione lenta e potrebbe richiedere da pochi secondi fino a un minuto. Tenerlo presente quando si applica il controllo Hyper-V a una quantità maggiore di macchine virtuali.

NOTA: al momento, il controllo Hyper-V è di sola lettura per la macchina virtuale in linea e non in linea. La capacità di pulire le infiltrazioni trovate sarà implementata in una fase successiva.

Convenzione sulla denominazione

Il modulo Controllo Hyper-V aderisce alla seguente convenzione di denominazione:
`NomeMacchinaVirtuale\DiscoX\VolumeY`

dove X è il numero del disco e Y è il numero del volume.
Ad esempio: `"Computer\Disco0\Volume1"`.

Il suffisso del numero viene aggiunto in base all'ordine di rilevamento che è identico a quello visualizzato in Gestione disco locale della VM.
Tale convezione di denominazione viene utilizzata nell'elenco strutturato ad albero delle destinazioni da controllare, sulla barra di avanzamento e anche nei file di rapporto.

Esecuzione di un controllo

Un controllo può essere eseguito in tre modi:

- Su richiesta: se si seleziona l'opzione Controllo Hyper-V nel menu di ESET Mail Security, verrà visualizzato un elenco di eventuali macchine virtuali disponibili da sottoporre al controllo. Si tratta di un elenco con struttura ad albero dove l'entità di livello più basso da sottoporre a controllo è un volume, il che significa che non è possibile scegliere una directory o file da sottoporre a controllo ma è necessario controllare almeno l'intero volume.
  Al fine di elencare i volumi disponibili, è necessario connettersi agli specifici dischi virtuali e questa operazione potrebbe richiedere alcuni secondi. Pertanto, l'opzione più veloce consiste nel contrassegnare una macchina virtuale o i relativi dischi da sottoporre al controllo.
  Dopo aver contrassegnato le macchine virtuali, i dischi o i volumi desiderati da sottoporre al controllo, fare clic sul pulsante Controlla.
- Tramite pianificazione attività
- Tramite ERA come un'attività client denominata Controllo server. La voce di livello inferiore da sottoporre a controllo è un disco di una macchina virtuale.

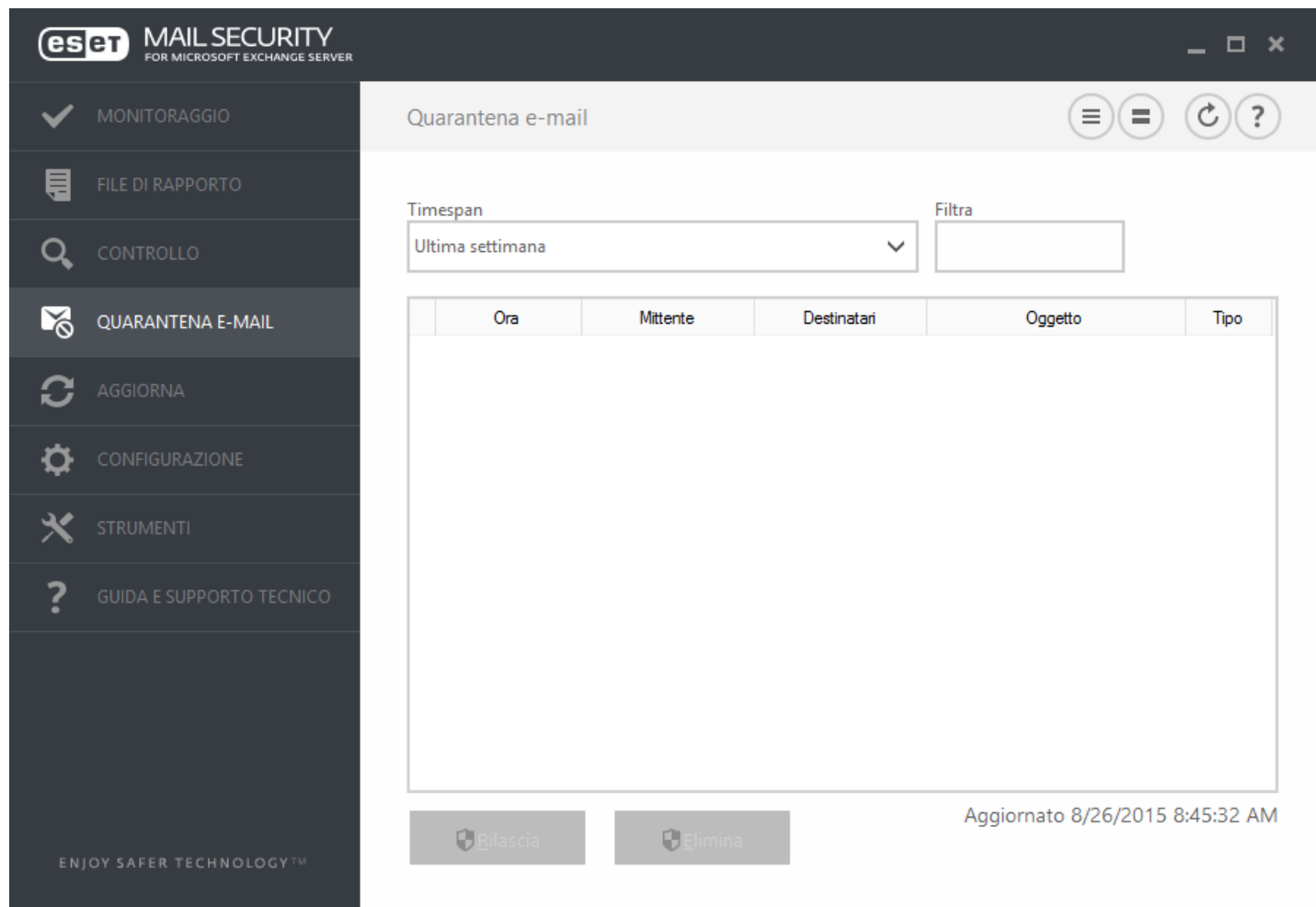
È possibile eseguire contemporaneamente più controlli Hyper-V.

Al termine del controllo, verrà visualizzata una notifica e un collegamento Mostra rapporto tramite il quale è possibile visualizzare i dettagli del controllo completato. Tutti i rapporti del controllo sono disponibili nella sezione File di rapporto di ESET Mail Security ma per poter visualizzare i relativi rapporti, è necessario scegliere Controllo Hyper-V dal menu a discesa.

Possibili problemi

- Quando si esegue il controllo di una macchina virtuale in linea, è necessario aver creato uno snapshot della macchina virtuale specifica e durante la creazione di uno snapshot alcune operazioni generiche della macchina virtuale potrebbero essere limitate o disattivate.
- Se una macchina virtuale non in linea viene sottoposta a controllo, non può essere attivata fino al termine del controllo.
- La Console di gestione di Hyper-V consente di denominare due macchine virtuali differenti in maniera identica e ciò rappresenta un problema quando si tenta di differenziare le macchine durante la consultazione dei rapporti del controllo.

4.4 Quarantena e-mail

La gestione quarantena e-mail è disponibile per tutti e tre i tipi di quarantena:

- Quarantena locale
- Casella di posta della quarantena
- Quarantena di MS Exchange

NOTA: l'Interfaccia Web della quarantena delle e-mail è un'alternativa alla gestione quarantena e-mail che consente all'utente di gestire gli oggetti delle e-mail in quarantena.

Filtraggio

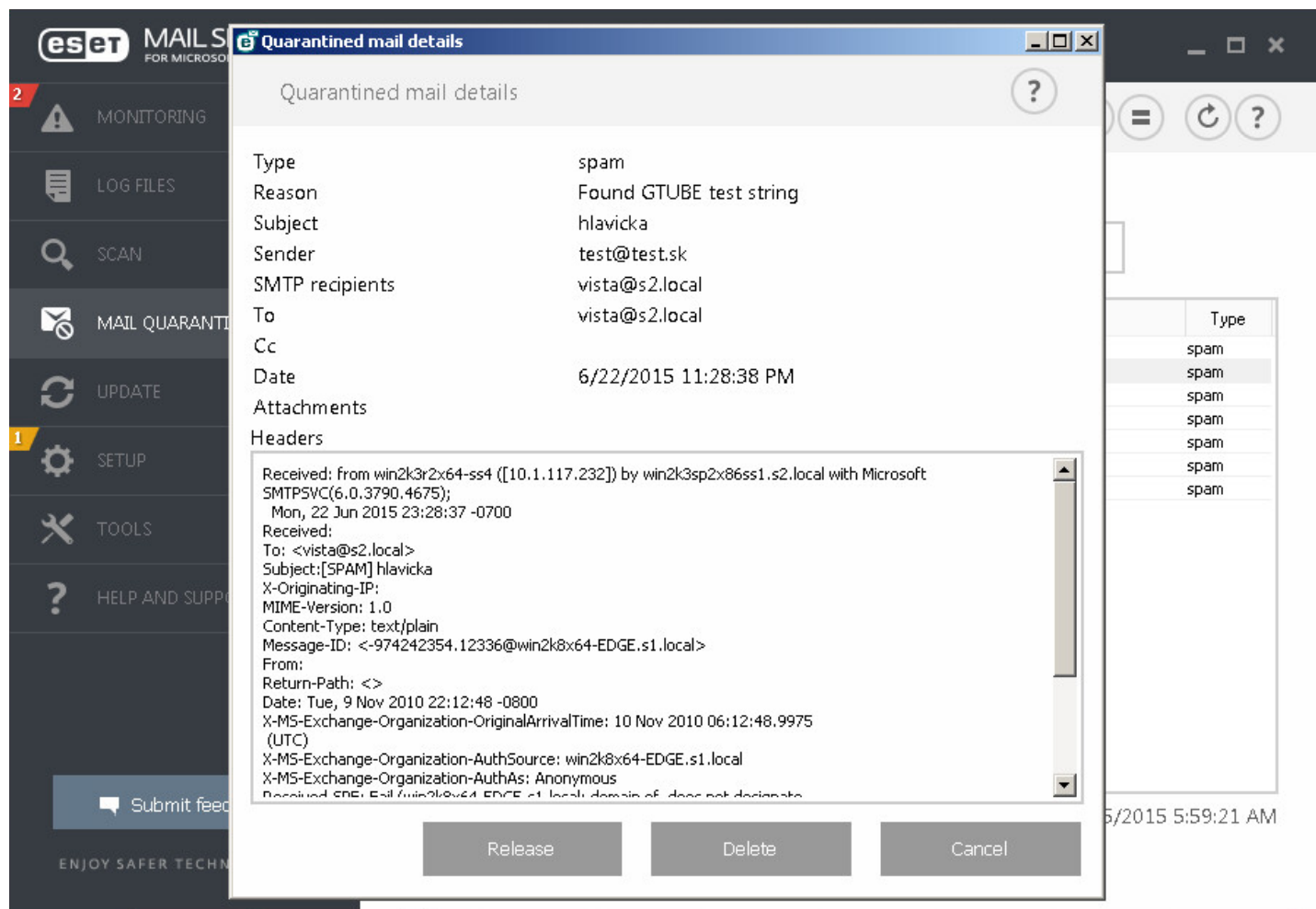
- **Intervallo temporale**: è possibile selezionare l'intervallo temporale a partire dal quale vengono visualizzate le e-mail (1 settimana per impostazione predefinita). Modificando l'intervallo temporale, gli oggetti della quarantena delle e-mail vengono ricaricati automaticamente.
- **Filtra**: è possibile utilizzare la casella di testo del filtraggio per filtrare le e-mail visualizzate (la ricerca viene eseguita in tutte le colonne).

NOTA: i dati della gestione quarantena e-mail non sono aggiornati automaticamente. Si consiglia pertanto di fare clic periodicamente su Aggiorna per visualizzare gli oggetti più recenti nella quarantena delle e-mail.

Azione

- ○ **Rilascia**: rilascia l'e-mail a uno o più destinatari originali utilizzando la directory Rispondi e la elimina dalla quarantena. Fare clic su **Sì** per confermare l'azione.
- ○ **Elimina**: elimina l'oggetto dalla quarantena. Fare clic su **Sì** per confermare l'azione.

Dettagli e-mail in quarantena: fare doppio clic sul messaggio in quarantena oppure fare clic con il pulsante destro del mouse e selezionare **Dettagli** per aprire una finestra popup contenente i dettagli relativi all'e-mail in quarantena. È possibile trovare anche ulteriori informazioni sull'e-mail nell'intestazione dell'e-mail RCF.

Le azioni sono disponibili anche dal menu contestuale. Se lo si desidera, fare clic su **Rilascia**, **Elimina** o **Elimina in modo permanente** per eseguire un'azione con un messaggio di posta elettronica in quarantena. Fare clic su **Sì** per confermare l'azione. Scegliendo **Elimina in modo permanente**, il messaggio verrà eliminato anche dal file system. Scegliendo invece **Elimina**, l'oggetto verrà rimosso dalla visualizzazione della gestione quarantena e-mail.

4.4.1 Dettagli messaggi e-mail posti in quarantena

In questa finestra sono contenute varie informazioni relative all'e-mail che è stata posta in quarantena, come **Tipo**, **Motivo**, **Oggetto**, **Mittente**, **Destinatari SMTP**, **A**, **Cc**, **Data**, **Allegati** e **Intestazioni**. È possibile selezionare, copiare e incollare le intestazioni, se necessario.

È possibile effettuare un'azione con le e-mail in quarantena mediante i pulsanti:

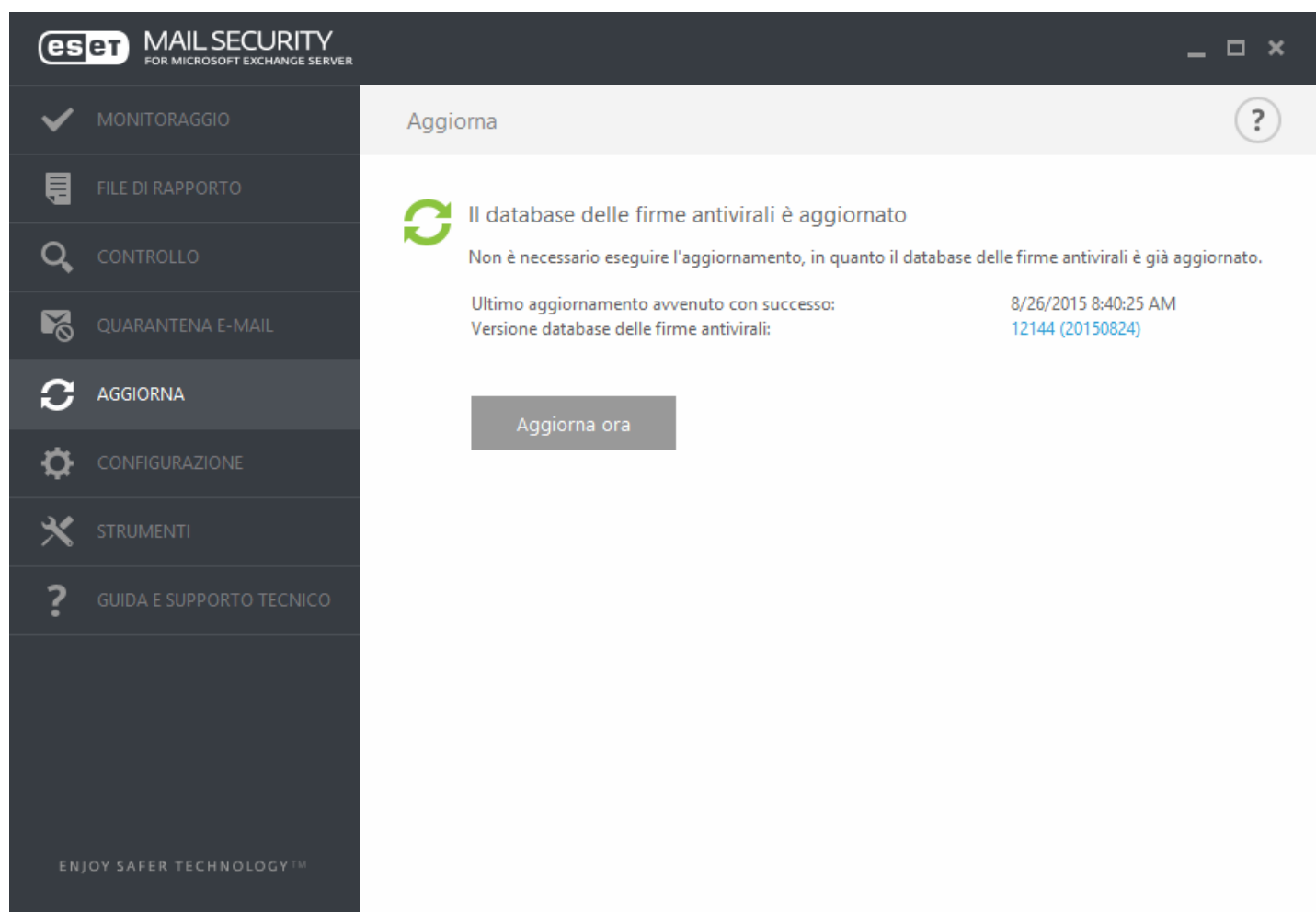
- ○ **Rilascia**: rilascia l'e-mail a uno o più destinatari originali utilizzando la directory Rispondi e la elimina dalla quarantena. Fare clic su **Sì** per confermare l'azione.
- ○ **Elimina**: elimina l'oggetto dalla quarantena. Fare clic su **Sì** per confermare l'azione.

Selezionando il pulsante **Annulla** viene chiusa la finestra contenente i dettagli sulle e-mail in quarantena.

4.5 Aggiornamento

L'aggiornamento periodico di ESET Mail Security rappresenta il metodo migliore per preservare il livello massimo di protezione del computer. Il modulo di aggiornamento garantisce l'aggiornamento ininterrotto del programma in due modi: attraverso l'aggiornamento rispettivamente del database delle firme antivirali e dei componenti del sistema.

Facendo clic su **Aggiorna** nella finestra principale del programma, è possibile visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento eseguito correttamente, e valutare l'eventuale necessità di un aggiornamento. Nella finestra principale sono inoltre contenute informazioni sulla versione del database delle firme antivirali. Questo indicatore numerico rappresenta un collegamento attivo al sito Web di ESET, in cui vengono riportate tutte le firme aggiunte nel corso dell'aggiornamento in questione.

Per avviare il processo di aggiornamento, fare clic su **Aggiorna adesso**. L'aggiornamento del database delle firme antivirali e dei componenti del programma costituisce un aspetto importante per garantire una protezione completa contro codici dannosi.

Ultimo aggiornamento riuscito: data dell'ultimo aggiornamento. Accertarsi che la data sia recente: ciò significa che il database delle firme antivirali è aggiornato.

Versione del database delle firme antivirali: numero del database delle firme antivirali, che rappresenta anche un collegamento attivo al sito Web ESET. Selezionare questa opzione per visualizzare un elenco di tutte le firme aggiunte in un aggiornamento specifico.

Processo di aggiornamento

Dopo aver selezionato **Aggiorna adesso**, verrà avviato il processo di download e verrà visualizzato lo stato di avanzamento dell'aggiornamento. Per interrompere l'aggiornamento, fare clic su **Annulla l'aggiornamento**.

Importante: in circostanze normali, quando gli aggiornamenti sono scaricati correttamente, nella finestra **Aggiorna** viene visualizzato il messaggio **Aggiornamento non necessario. Il database delle firme antivirali è aggiornato**. In caso contrario, il programma è obsoleto ed è maggiormente esposto alle infezioni. Aggiornare il database delle firme antivirali appena possibile. In caso contrario, viene visualizzato uno dei seguenti messaggi:

Il database delle firme antivirali è obsoleto: questo errore viene visualizzato dopo diversi tentativi non riusciti di aggiornamento del database delle firme antivirali. Si consiglia di controllare le impostazioni di aggiornamento. Spesso questo errore viene visualizzato perché i dati di autenticazione non vengono immessi correttamente o le impostazioni di connessione sono errate.

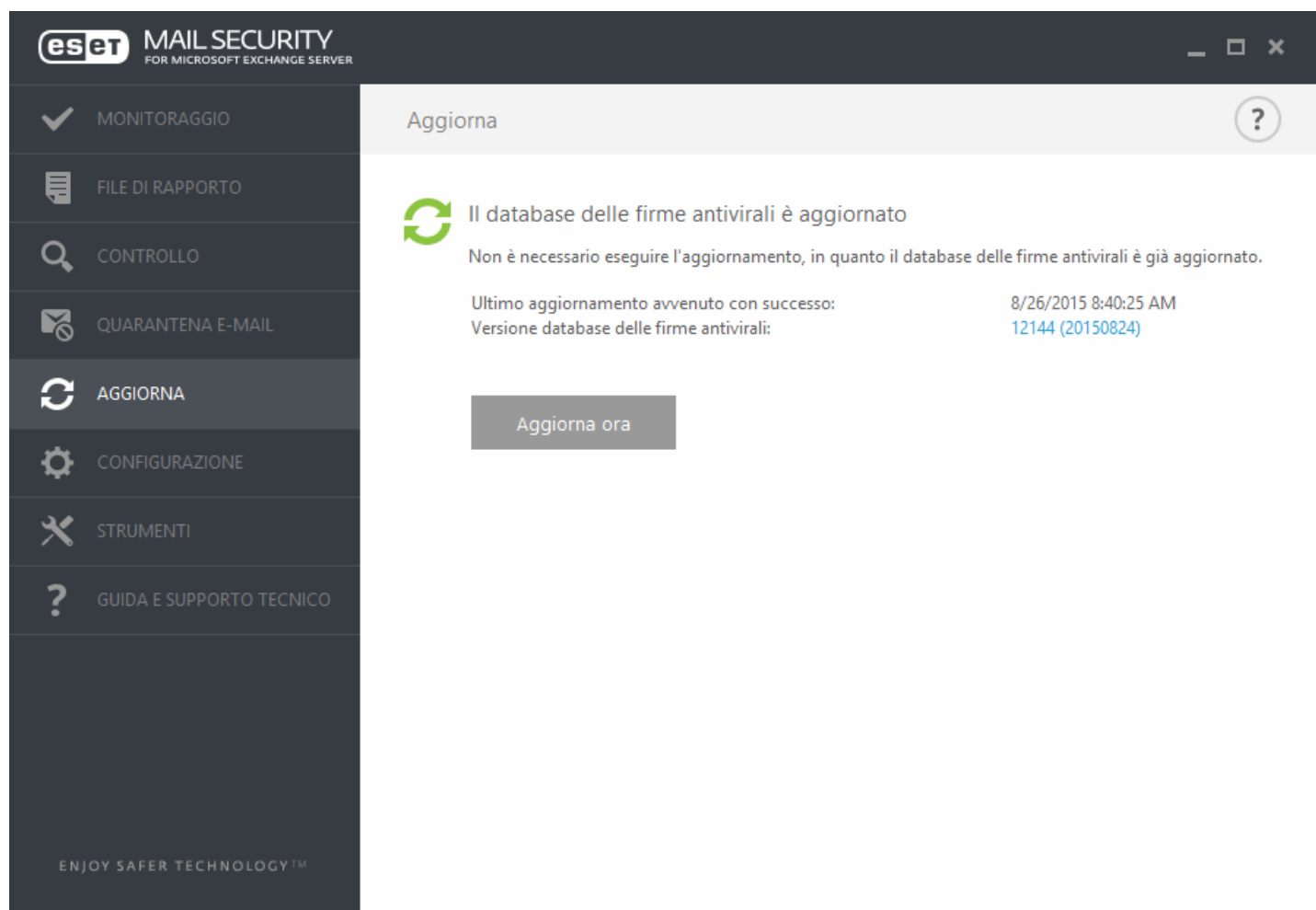
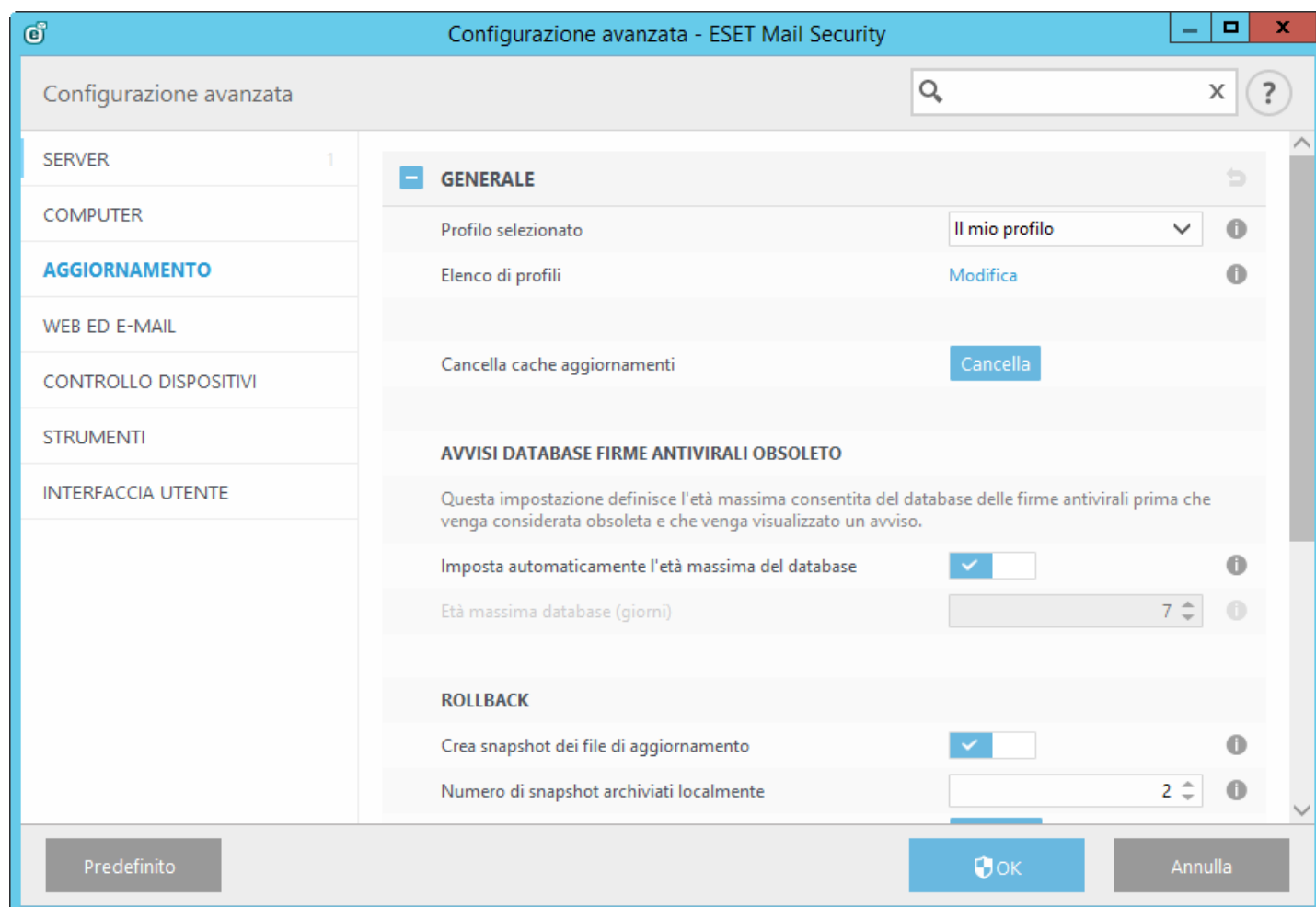
Il messaggio di notifica precedente è correlato ai due messaggi che seguono, relativi ad aggiornamenti non riusciti (**Aggiornamento del database delle firme antivirali non riuscito**):

Licenza non valida: la chiave di licenza non è stata inserita correttamente durante la configurazione dell'aggiornamento. Si consiglia di verificare i dati di autenticazione. La finestra configurazione avanzata (premere F5 sulla tastiera) contiene opzioni di aggiornamento aggiuntive. Fare clic su **Guida e supporto tecnico** > **Gestisci licenza** nel menu principale per inserire una nuova chiave di licenza.

Si è verificato un errore durante il download dei file di aggiornamento: questo errore potrebbe essere causato da Impostazioni di connessione Internet non corrette. Si consiglia di verificare la connettività Internet aprendo un qualsiasi sito Web nel browser. Se il sito Web non si apre, è possibile che la connessione Internet non sia presente o che si siano verificati problemi di connettività nel computer in uso. Se la connessione Internet non è attiva, contattare il proprio Provider di servizi Internet (ISP).

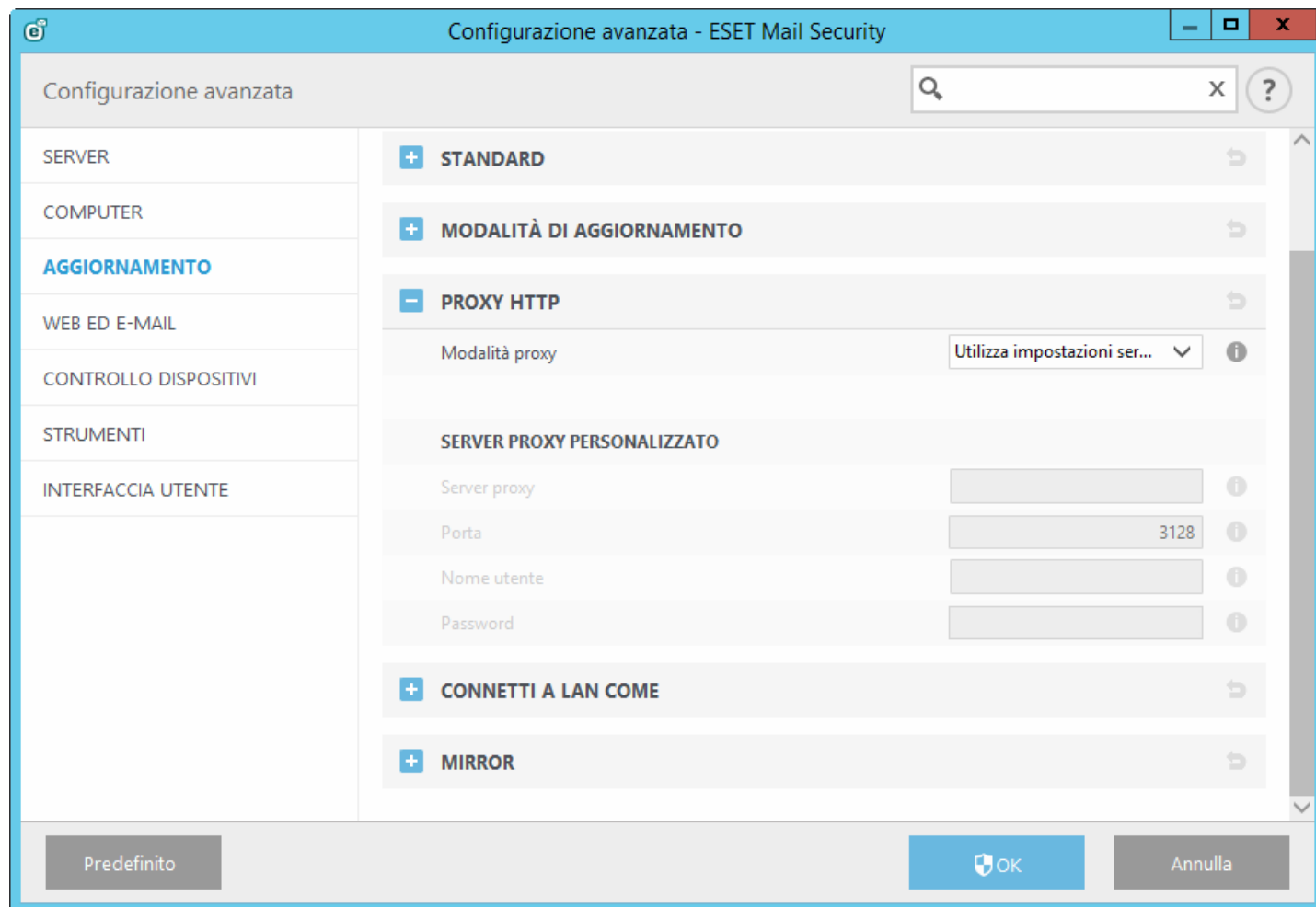
NOTA: per ulteriori informazioni, consultare questo articolo della Knowledge Base ESET.

4.5.1 Configurazione dell'aggiornamento del database delle firme antivirali

L'aggiornamento del database delle firme antivirali e dei componenti del programma costituisce un aspetto importante per garantire una protezione completa contro codici dannosi. È opportuno prestare attenzione alla configurazione e al funzionamento di tali risorse. Nel menu principale, accedere a **Aggiorna**, quindi fare clic su **Aggiorna ora** per verificare la disponibilità di un database delle firme antivirali più recente.

È possibile configurare le impostazioni di aggiornamento dalla finestra Configurazione avanzata (premere il tasto F5 sulla tastiera). Per configurare le opzioni di aggiornamento avanzate, come ad esempio la modalità di aggiornamento, l'accesso al server proxy, la connessione LAN e le impostazioni relative alle copie delle firme antivirali (mirror), fare clic su **Aggiorna** nella finestra **Configurazione avanzata** sulla sinistra. In caso di problemi di aggiornamento, fare clic su **Cancella cache** per eliminare la cartella dei file di aggiornamento temporanei. Per impostazione predefinita, il menu **Server di aggiornamento** è impostato su **SELEZIONE AUTOMATICA**. **SELEZIONE AUTOMATICA** indica che il server dal quale vengono scaricati gli aggiornamenti del database delle firme antivirali viene scelto automaticamente. È consigliabile conservare l'opzione predefinita selezionata. Se non si desidera visualizzare la notifica sulla barra delle applicazioni del sistema nell'angolo in basso a destra della schermata, selezionare **Disattiva visualizzazione notifiche relative agli aggiornamenti eseguiti correttamente**.

Per garantire un livello di funzionalità ottimale, è fondamentale che il programma venga aggiornato automaticamente. Questa operazione può essere eseguita soltanto dopo aver inserito la **Chiave di licenza** corretta in **Guida e supporto tecnico** > **Attiva licenza.**

In caso di mancata attivazione del prodotto in seguito all'installazione, è possibile eseguire l'operazione in qualsiasi momento. Per ulteriori informazioni sull'attivazione, consultare Come fare per attivare ESET Mail Security e inserire i dati di licenza ricevuti insieme al prodotto di protezione ESET nella finestra Dettagli licenza.

4.5.2 Configurazione del server proxy per gli aggiornamenti

In caso di utilizzo di un server proxy per la connessione a Internet su un sistema su cui è installato ESET Mail Security, le impostazioni del proxy devono essere configurate in Configurazione avanzata. Per accedere alla finestra di configurazione del server proxy, premere F5 per aprire la finestra Configurazione avanzata e fare clic su **Aggiornamento** > **Proxy HTTP**. Selezionare **Connessione tramite un server proxy**dal menu a discesa **Modalità proxy** e inserire i dettagli del server proxy: **Server proxy** (indirizzo IP), numero di **Porta** e **Nome utente** e **Password** (se disponibili).

In caso di dubbi sulle informazioni relative al server proxy, tentare di recuperare automaticamente le relative impostazioni selezionando **Utilizza impostazioni server proxy globali** dall'elenco a discesa.

i **NOTA:** le opzioni del server proxy potrebbero essere diverse in base ai diversi profili di aggiornamento. In questo caso, configurare i diversi profili di aggiornamento nella finestra Configurazione avanzata facendo clic su **Aggiornamento** > **Profilo**.

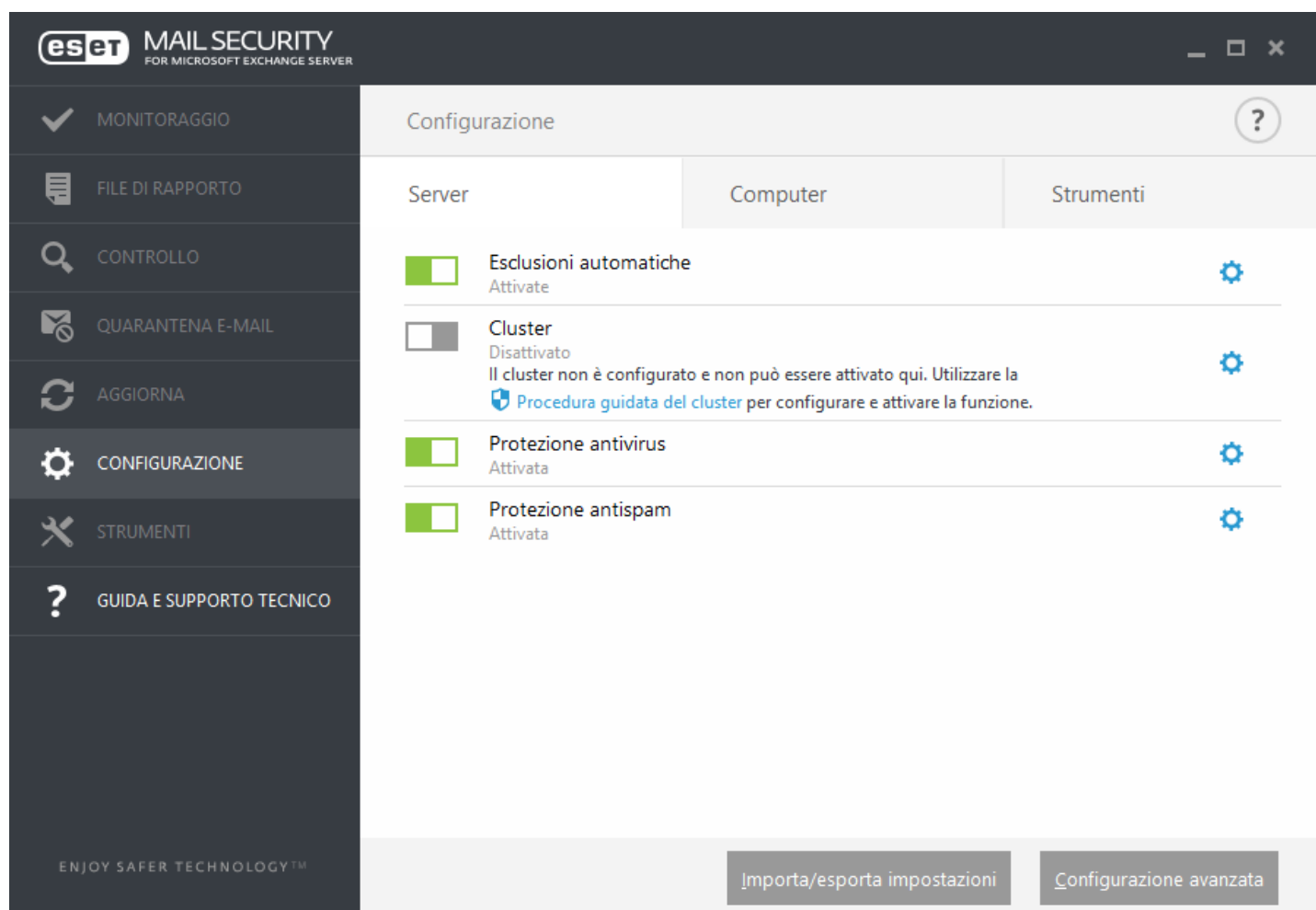
4.6 Configurazione

Il menu Configurazione è formato da tre schede:

- Server
- Computer
- Strumenti

4.6.1 Server

ESET Mail Security assicura la protezione del server con funzionalità essenziali quali: antivirus e antispyware, scudo residente (protezione in tempo reale), protezione accesso Web e protezione client di posta. Ulteriori informazioni su ciascun tipo di protezione sono disponibili in ESET Mail Security: protezione computer.

- Esclusioni automatiche: questa funzione identifica le applicazioni server e i file del sistema operativo server critici e li aggiunge automaticamente all'elenco di Esclusioni. Questa funzionalità riduce al minimo il rischio di potenziali conflitti e migliora le prestazioni generali del server quando è in esecuzione il software antivirus.
- Per configurare ESET Cluster, fare clic su **Procedura guidata cluster**. Per informazioni dettagliate sulle modalità di configurazione di ESET Cluster tramite la procedura guidata, fare clic qui.

Se si desidera impostare opzioni più dettagliate, fare clic su **Configurazione avanzata** oppure premere **F5**.

Nella parte inferiore della finestra di configurazione sono disponibili ulteriori opzioni. Per caricare i parametri di configurazione mediante un file di configurazione *.xml* o per salvare i parametri di configurazione correnti in un file di configurazione, utilizzare **Importa/esporta impostazioni**. Per ulteriori informazioni, consultare Importa/esporta impostazioni.

4.6.2 Computer

ESET Mail Security contiene tutti i componenti necessari per garantire un livello di protezione adeguato di un server come ad esempio un computer. Ciascun componente offre un tipo specifico di protezione, tra cui: antivirus e antispyware, protezione file system in tempo reale, accesso Web, client di posta, protezione Anti-Phishing e così via.

La sezione **Computer** è disponibile sotto a **Configurazione** > **Computer**. Sarà possibile visualizzare un elenco di componenti da attivare/disattivare utilizzando il pulsante . Per configurare le impostazioni di uno specifico elemento, fare clic sulla rotella . Per la **Protezione file system in tempo reale** è inoltre disponibile un'opzione che consente di **Modificare le esclusioni**, che aprirà la finestra di configurazione delle Esclusioni in cui è possibile

escludere file e cartelle dal controllo.

Sospendi protezione antivirus e antispyware: tutte le volte che viene disattivata temporaneamente la protezione antivirus e antispyware, è possibile selezionare il periodo di tempo per il quale si desidera disattivare il componente selezionato utilizzando il menu a discesa e facendo clic su **Applica** per disattivare il componente di protezione. Per riattivare la protezione, fare clic su **Attiva protezione antivirus e antispyware**.

Il modulo **Computer** consente all'utente di attivare/disattivare e configurare i seguenti componenti:

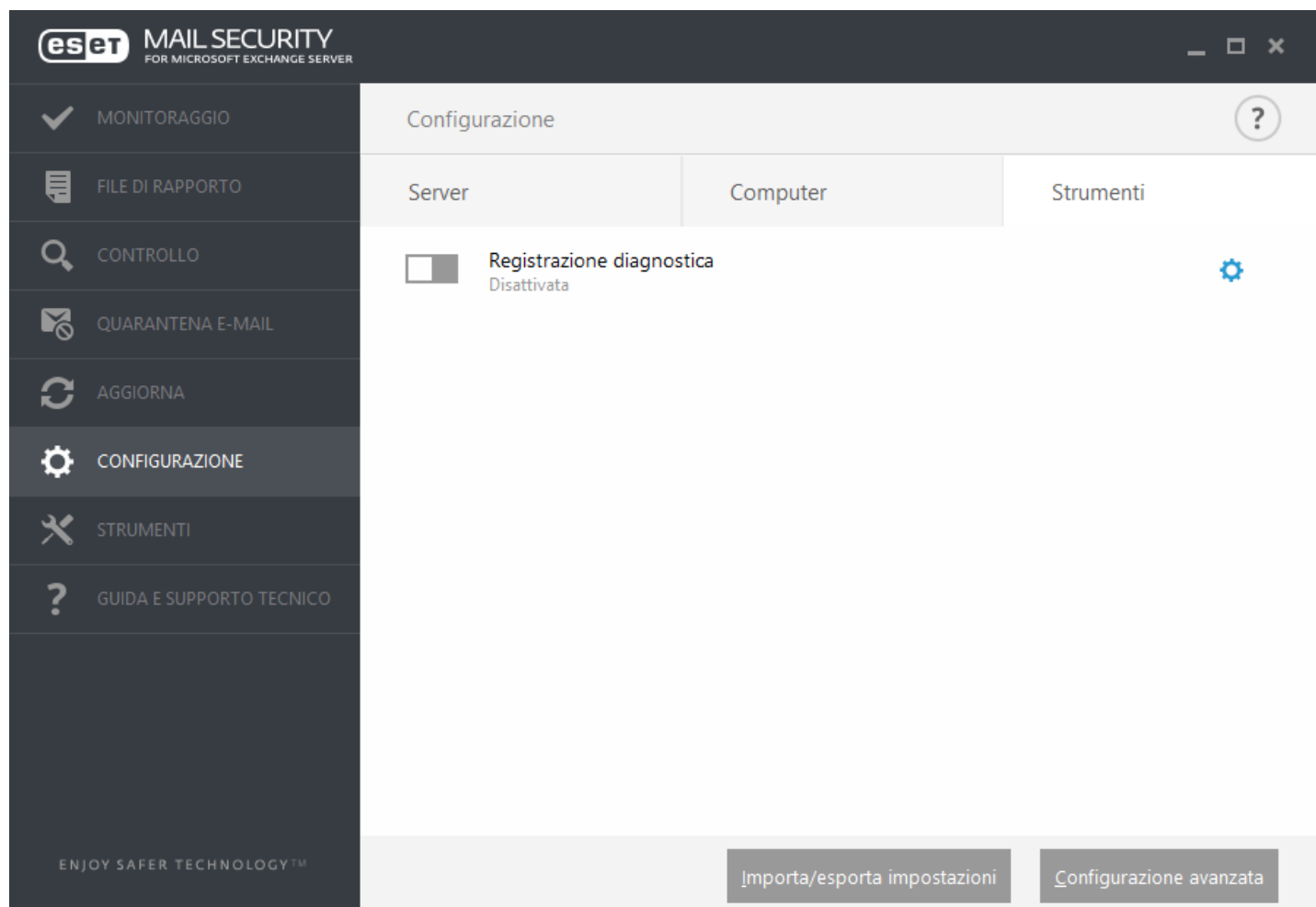
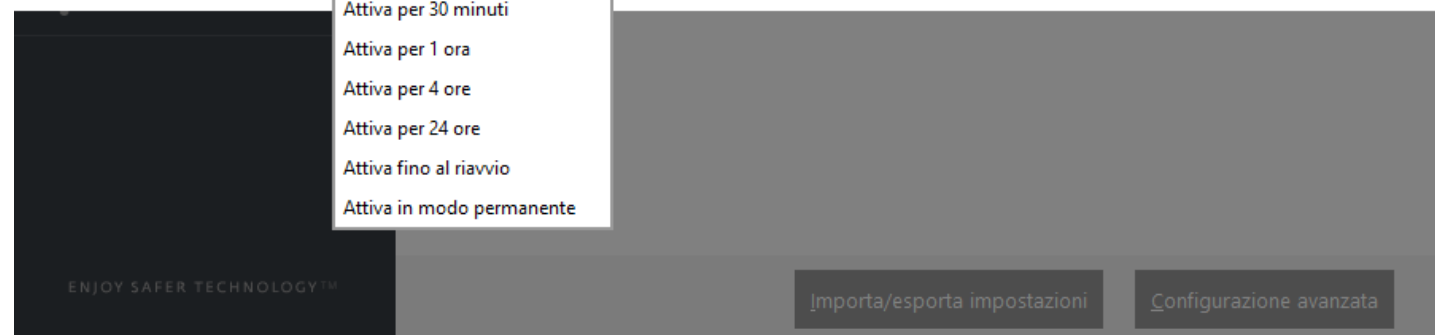
- **Protezione file system in tempo reale**: tutti i file vengono sottoposti a controllo per la ricerca di codici dannosi al momento dell'apertura, creazione o esecuzione sul computer.
- **Protezione documenti**: la funzione protezione documenti consente di eseguire il controllo dei documenti di Microsoft Office prima della loro apertura e dei file scaricati automaticamente da Internet Explorer, ad esempio gli elementi di Microsoft ActiveX.
- **Controllo dispositivi:** questo modulo consente all'utente di controllare, bloccare o regolare le estensioni dei filtri o delle autorizzazioni e di definire la capacità dell'utente di accedere e di utilizzare un determinato dispositivo.
- **HIPS**: il sistema HIPS monitora gli eventi che avvengono all'interno del sistema operativo e reagisce in base a un set personalizzato di regole.
- **Modalità presentazione**: funzionalità per gli utenti che desiderano utilizzare il software senza interruzioni, non essere disturbati dalle finestre popup e ridurre al minimo l'utilizzo della CPU. Dopo aver attivato la Modalità presentazione, l'utente riceverà un messaggio di avviso (potenziale rischio per la protezione) e la finestra principale del programma diventerà di colore arancione.
- **Protezione Anti-Stealth**: consente di rilevare programmi pericolosi, ad esempio rootkit, che riescono a nascondersi dal sistema operativo. Ciò significa che non è possibile rilevarli utilizzando le normali tecniche di testing.
- **Protezione accesso Web**: se questa opzione è attiva, viene eseguito il controllo di tutto il traffico HTTP o HTTPS per la ricerca di software dannoso.
- **Protezione client di posta**: monitora le comunicazioni ricevute mediante il protocollo POP3 e IMAP.
- **Protezione Anti-Phishing**: protegge l'utente da tentativi di acquisizione di password, dati bancari e altre informazioni sensibili da parte di siti Web illegittimi camuffati da siti legittimi.

i **NOTA:** la Protezione documenti è disattivata per impostazione predefinita. Se lo si desidera, è possibile attivarla facilmente facendo clic sull'icona del pulsante.

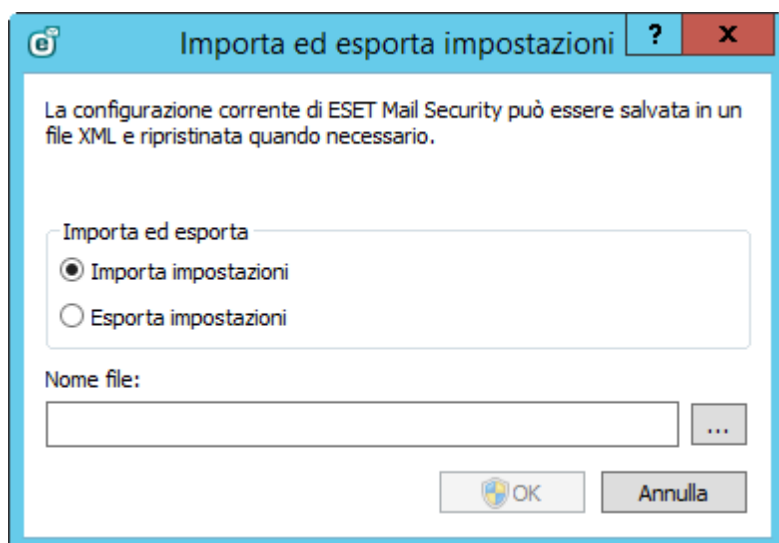
Nella parte inferiore della finestra di configurazione sono disponibili ulteriori opzioni. Per caricare i parametri di configurazione mediante un file di configurazione *.xml* o per salvare i parametri di configurazione correnti in un file di configurazione, utilizzare **Importa/esporta impostazioni**. Per ulteriori informazioni, consultare Importa/esporta impostazioni.

Se si desidera impostare opzioni più dettagliate, fare clic su **Configurazione avanzata** oppure premere **F5**.

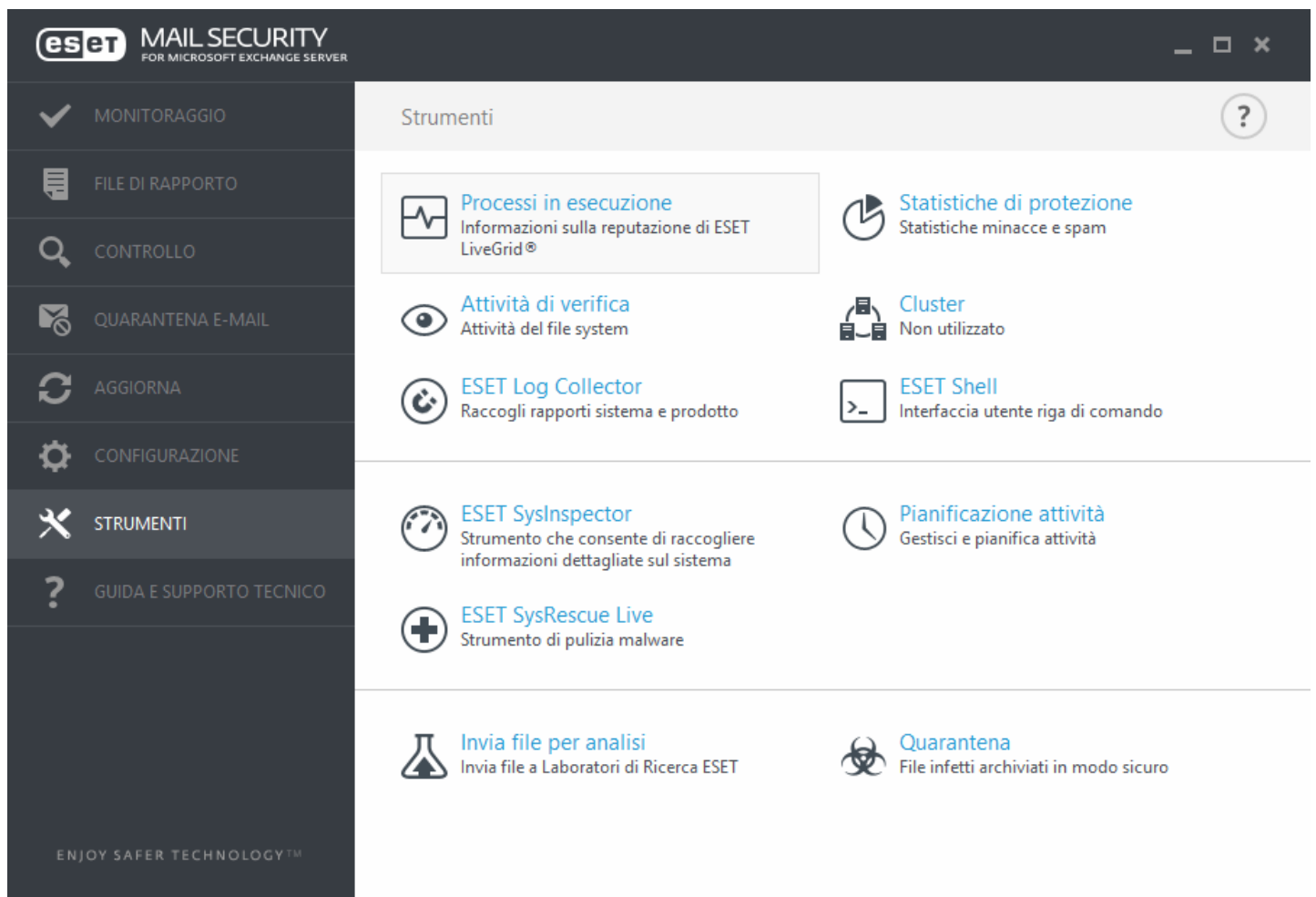
4.6.3 Strumenti

Registrazione diagnostica: configura i componenti che scriveranno rapporti di diagnostica in caso di attivazione della registrazione diagnostica. Quando si seleziona il pulsante per attivare la registrazione diagnostica, è possibile scegliere l'intervallo di tempo in cui sarà attivata (10 minuti, 30 minuti, 1 ora, 4 ore, 24 ore, fino al successivo riavvio del server o in modo permanente). I componenti non menzionati in questa scheda scrivono sempre rapporti di diagnostica.

- **Attiva** registrazione diagnostica per il periodo di tempo selezionato.

4.6.4 Importa ed esporta impostazioni

La funzione di importazione ed esportazione della configurazione di ESET Mail Security è disponibile sotto a **Configurazione** facendo clic su **Importa/Esporta impostazioni**.

Le opzioni di importazione e di esportazione utilizzano entrambe il tipo di file XML. Le funzioni di importazione e di esportazione sono utili se si desidera eseguire il back-up della configurazione corrente di ESET Mail Security. È possibile utilizzarle in un secondo momento per applicare le stesse impostazioni ad altri computer.

4.7 Strumenti

Il menu Strumenti include moduli che consentono di semplificare l'amministrazione del programma e che offrono opzioni supplementari. Sono compresi gli strumenti seguenti:

- Processi in esecuzione
- Attività di verifica
- ESET Log Collector
- Statistiche di protezione
- Cluster
- ESET Shell
- ESET SysInspector
- ESET SysRescue Live
- Pianificazione attività
- Invia campione per analisi
- Quarantena

4.7.1 Processi in esecuzione

I processi in esecuzione consentono di visualizzare i programmi o processi in esecuzione sul computer e inviare informazioni tempestive e costanti a ESET sulle nuove infiltrazioni. ESET Mail Security fornisce informazioni dettagliate sui processi in esecuzione allo scopo di proteggere gli utenti che utilizzano la tecnologia ESET Live Grid.

Livello di rischio: nella maggior parte dei casi, ESET Mail Security e la tecnologia ESET Live Grid assegnano livelli di rischio agli oggetti (file, processi, chiavi di registro, ecc.), utilizzando una serie di regole euristiche che esaminano le caratteristiche di ciascun oggetto valutandone le potenzialità come attività dannosa. Sulla base di tali euristiche, agli oggetti viene assegnato un livello di rischio da 1: non a rischio (verde) a 9: a rischio (rosso).

Processo: nome immagine del programma o del processo attualmente in esecuzione sul computer. Per visualizzare tutti i processi in esecuzione sul computer è inoltre possibile utilizzare Windows Task Manager. Per aprire il Task Manager, fare clic con il pulsante destro del mouse su un'area vuota della barra delle attività, quindi scegliere Task Manager oppure premere **Ctrl+Maiusc+Esc** sulla tastiera.

PID: ID dei processi in esecuzione sui sistemi operativi Windows.

NOTA: le applicazioni note contrassegnate come Non a rischio (verde) sono definite pulite (inserite nella whitelist) e saranno escluse dal controllo in modo da aumentare la velocità di esecuzione del controllo del computer su richiesta o della protezione file system in tempo reale sul computer.

Numero di utenti: numero di utenti che utilizzano una determinata applicazione. Queste informazioni vengono raccolte mediante la tecnologia ESET Live Grid.

Ora di rilevamento: ora in cui l'applicazione è stata rilevata dalla tecnologia ESET Live Grid.

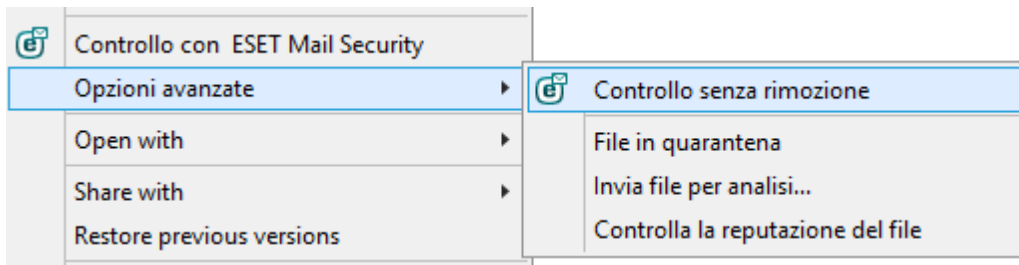
NOTA: se un'applicazione è contrassegnata con un livello di rischio Sconosciuto (arancione), non si tratta necessariamente di software dannoso. In genere si tratta di una nuova applicazione. In caso di dubbi sul file, utilizzare la funzione Invia campione per analisi per inviare il file al laboratorio antivirus ESET. Se il file si rivela essere un'applicazione dannosa, il suo rilevamento verrà aggiunto a uno degli aggiornamenti successivi del

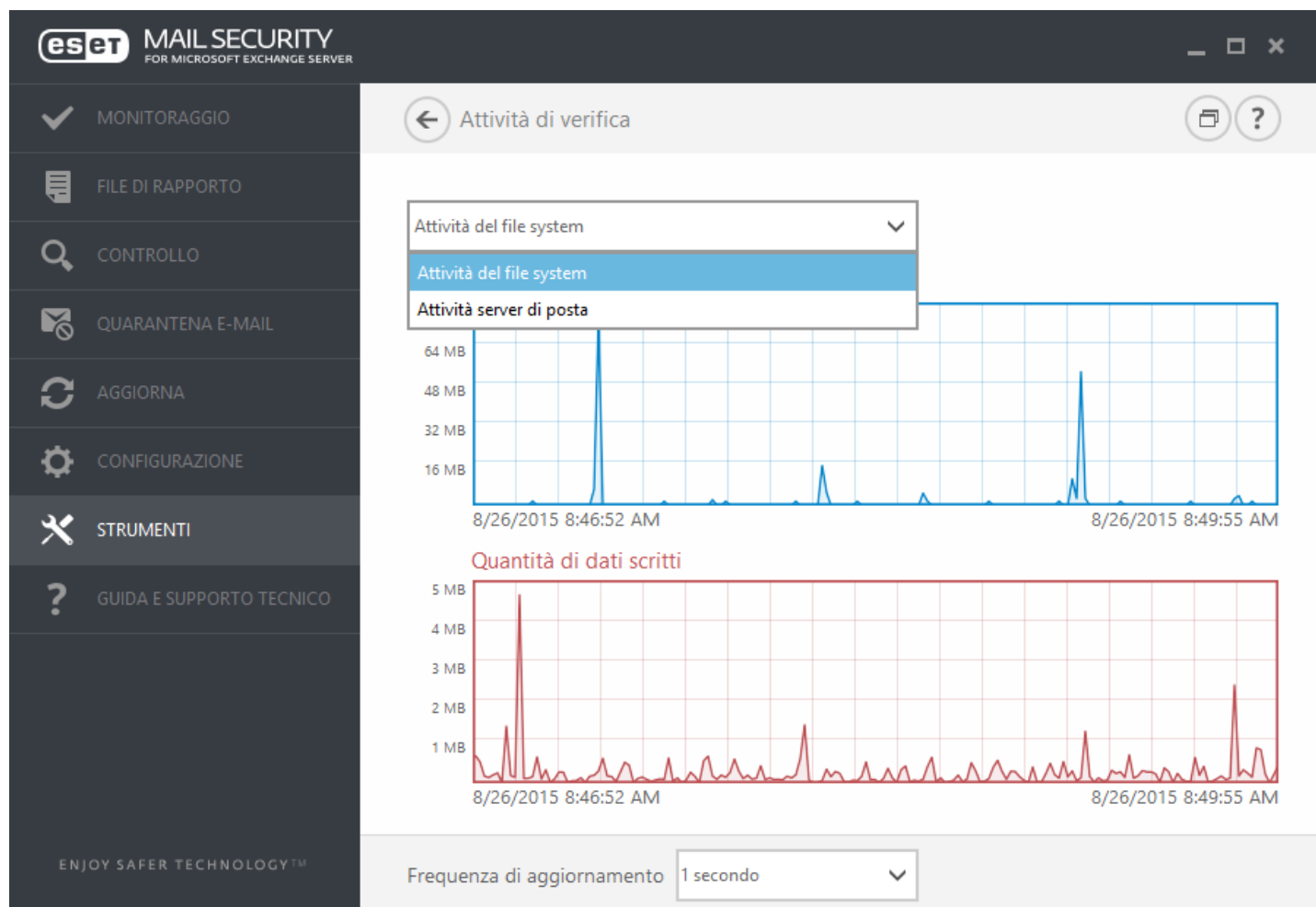
database delle firme antivirali.

Nome applicazione: nome specifico di un programma a cui appartiene tale processo.

Fare clic sulla parte inferiore di una determinata applicazione per visualizzare le seguenti informazioni nella parte inferiore della finestra:

- **Percorso**: posizione di un'applicazione sul computer.
- **Dimensione**: dimensione del file in kB (kilobyte) o MB (megabyte).
- **Descrizione**: caratteristiche del file basate sulla descrizione ottenuta dal sistema operativo.
- **Società**: nome del fornitore o del processo applicativo.
- **Versione**: informazioni estrapolate dall'autore dell'applicazione.
- **Prodotto**: nome dell'applicazione e/o nome commerciale.
- **Creato il**: data e ora della creazione di un'applicazione.
- **Modificato il**: data e ora dell'ultima modifica apportata a un'applicazione.

NOTA: la reputazione può essere controllata anche sui file che non agiscono come programmi/processi in esecuzione: contrassegnare i file che si desidera controllare, fare clic con il pulsante destro del mouse su di essi e nel menu contestuale selezionare **Opzioni avanzate** > **Controlla la reputazione del file tramite ESET Live Grid**.

4.7.2 Attività di verifica

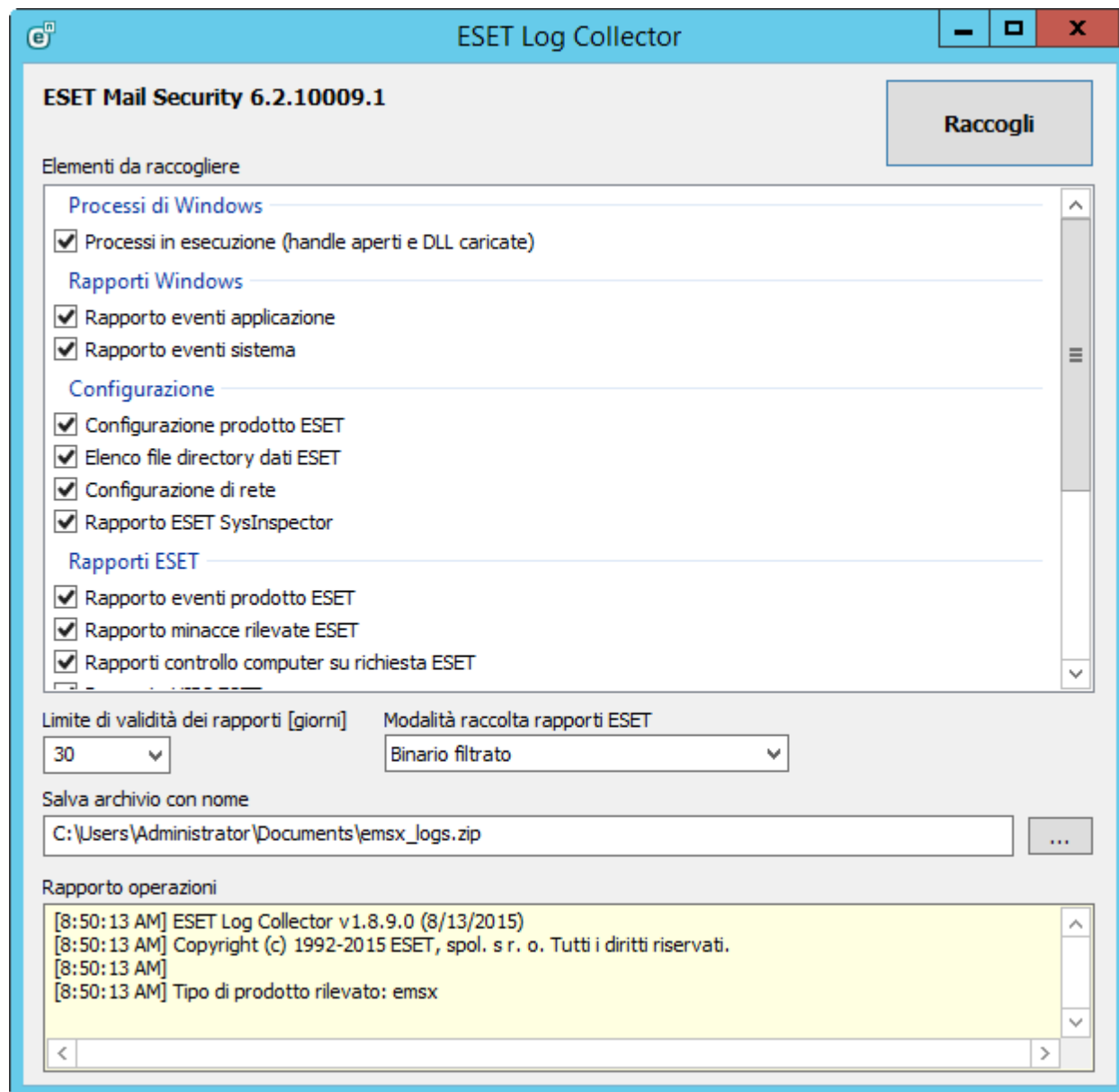
Per visualizzare l'**Attività del file system** corrente in un grafico, fare clic su **Strumenti** > **Attività di verifica**. Consente all'utente di visualizzare la quantità di dati letti e scritti nel sistema in due diversi grafici. Nella parte inferiore del grafico è presente una linea cronologica che registra in tempo reale le attività del file system in base all'intervallo di tempo selezionato. Per modificare l'intervallo di tempo, selezionarlo nel menu a discesa **Frequenza di aggiornamento**.

Sono disponibili le seguenti opzioni:

- **1 secondo** : il grafico si aggiorna ogni secondo e l'intervallo di tempo copre gli ultimi 10 minuti.
- **1 minuto (ultime 24 ore)** : il grafico si aggiorna ogni minuto e l'intervallo di tempo copre le ultime 24 ore.
- **1 ora (ultimo mese)** : il grafico si aggiorna ogni ora e l'intervallo di tempo copre l'ultimo mese.
- **1 ora (mese selezionato)** : il grafico si aggiorna ogni ora e l'intervallo di tempo copre il mese selezionato. Fare clic sul pulsante **Cambia mese** per fare un'altra scelta.

L'asse verticale del **grafico dell'**Attività del file system rappresenta il numero di dati letti (blu) e scritti (rosso). Entrambi i valori sono espressi in KB (kilobyte)/MB/GB. Facendo scorrere il mouse sui dati letti o scritti nella didascalia sottostante il grafico, è possibile visualizzare unicamente i dati relativi a quella specifica attività.

4.7.3 ESET Log Collector

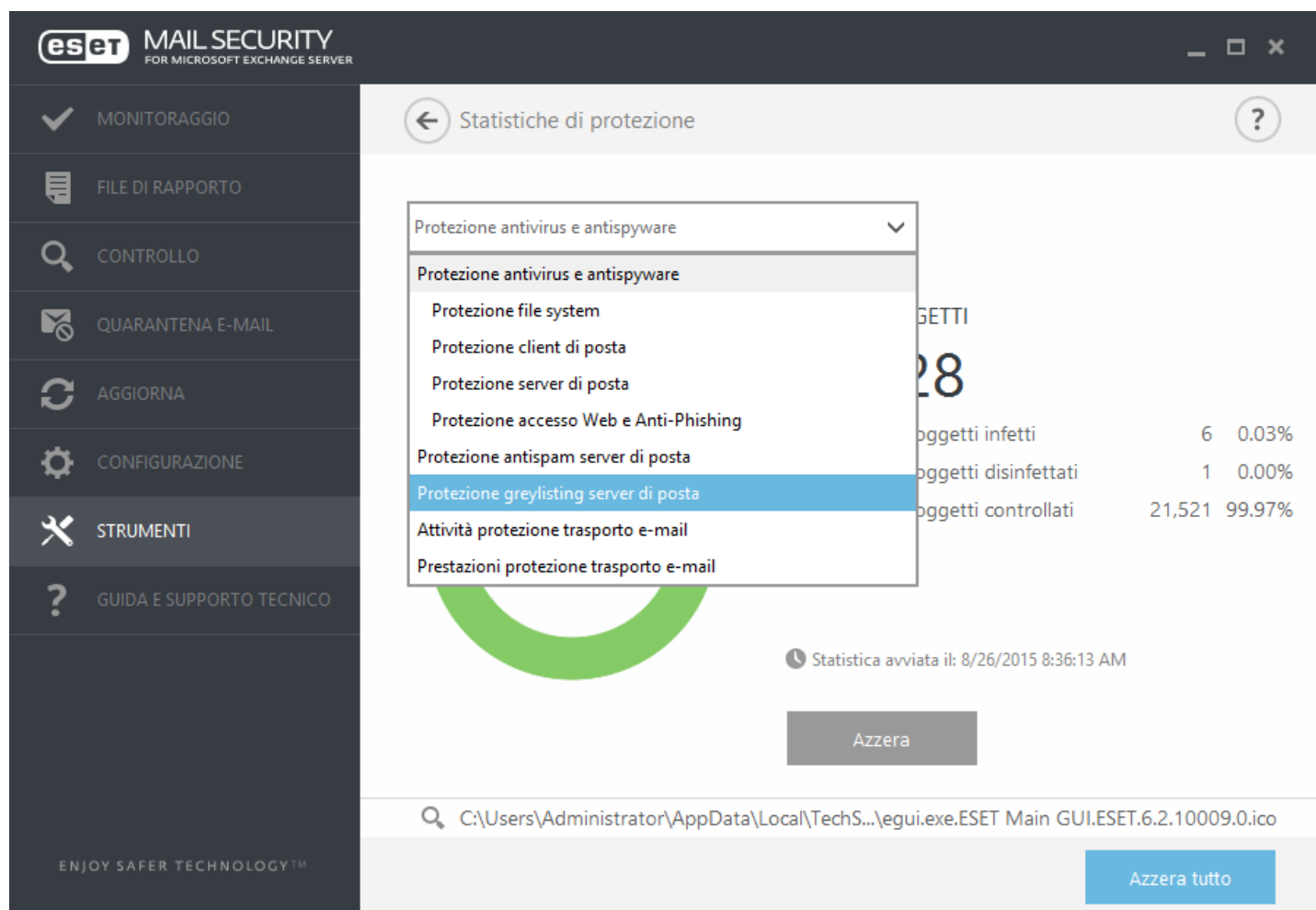
ESET Log Collector è un'applicazione che raccoglie automaticamente informazioni, come ad esempio i dati sulle configurazioni e i rapporti dal server allo scopo di risolvere i problemi in modo più rapido. Nel caso in cui si apra un caso con il Supporto tecnico ESET, all'utente verrà talvolta richiesto di fornire i rapporti archiviati sul computer. ESET Log Collector faciliterà la raccolta delle informazioni necessarie.

È possibile accedere a ESET Log Collector dal menu principale facendo clic su **Strumenti** > **ESET Log Collector**.

Selezionare le caselle di controllo relative ai rapporti che si desidera raccogliere. In caso di dubbi sulle caselle da selezionare, lasciarle tutte selezionate, come da impostazione predefinita. Specificare il percorso in cui si desiderano salvare i file da archiviare, quindi fare clic su **Salva**. Il nome del file dell'archivio è già predefinito. Fare clic su **Raccogli**.

Durante la raccolta, in basso viene visualizzata la finestra del rapporto operazioni per consentire di visualizzare l'operazione attualmente in corso. Al termine della raccolta, verranno visualizzati tutti i file raccolti e archiviati. Ciò significa che la raccolta è stata completata e che il file dell'archivio (ad esempio, `emsx_logs.zip`) è stato salvato nel percorso specificato.

Per ulteriori informazioni su ESET Log Collector e sull'elenco dei file raccolti da ESET Log Collector, consultare la Knowledge Base ESET.

4.7.4 Statistiche di protezione

Per visualizzare un grafico dei dati statistici relativi ai moduli di protezione in ESET Mail Security, fare clic su **Strumenti** > **Statistiche di protezione**. Selezionare il modulo di protezione desiderato dal menu a discesa **Statistiche** per visualizzare il grafico e la legenda corrispondenti. Spostare il mouse su una voce della legenda per visualizzarne i dati nel grafico.

Sono disponibili i seguenti grafici statistici:

- **Protezione antivirus e antispyware**: consente di visualizzare il numero complessivo di oggetti infetti e puliti.
- **Protezione file system**: consente di visualizzare solo gli oggetti che sono stati scritti o letti sul file system.
- **Protezione client di posta**: consente di visualizzare solo gli oggetti inviati o ricevuti dai client di posta.
- **Protezione server di posta**: consente di visualizzare le statistiche del server di posta antivirus e antispyware.
- **Protezione accesso Web e Anti-Phishing**: consente di visualizzare solo gli oggetti scaricati dai browser Web.
- **Protezione antispam server di posta**: consente di visualizzare la cronologia delle statistiche antispam dall'ultimo avvio.
- **Protezione greylist server di posta**: include le statistiche antispam generate mediante il metodo greylist.
- **Attività protezione trasporto e-mail**: consente di visualizzare gli oggetti verificati/bloccati/eliminati dal server di posta.
- **Prestazioni protezione trasporto e-mail**: consente di visualizzare i dati elaborati da VSAPI/Agente di trasporto in B/s.
- **Attività protezione database casella di posta**: consente di visualizzare gli oggetti elaborati da VSAPI (numero di oggetti **verificati**, **messi in quarantena** ed **eliminati**).
- **Prestazioni protezione database casella di posta**: consente di visualizzare i dati elaborati da VSAPI (numero di medie differenti per **Oggi**e per gli **Ultimi 7 giorni** e di medie **Dall'ultimo ripristino**).

Accanto al grafico delle statistiche è possibile visualizzare il numero di oggetti sottoposti a controllo, infetti, sottoposti a pulizia e puliti. Fare clic su **Reimposta** per cancellare le informazioni statistiche oppure su **Reimposta tutto** per cancellare e rimuovere tutti i dati esistenti.

4.7.5 Cluster

ESET Cluster è un'infrastruttura di comunicazione P2P della gamma di prodotti ESET per Microsoft Windows Server.

Questa infrastruttura consente ai prodotti server ESET di comunicare tra loro e scambiare dati quali configurazioni e notifiche, oltre a sincronizzare i dati necessari per il corretto funzionamento di un gruppo di istanze del prodotto. Un esempio potrebbe essere un gruppo di nodi in un cluster di failover Windows o cluster NLB (Network Load Balancing) con il prodotto ESET installato dove è richiesta la stessa configurazione del prodotto sull'intero cluster. ESET Cluster assicura questo livello di coerenza tra le istanze.

La pagina di stato di ESET Cluster è accessibile dal menu principale in **Strumenti** > **Cluster** (se configurato correttamente) e presenta le seguenti caratteristiche:

Per configurare ESET Cluster, fare clic su **Procedura guidata cluster...** Per informazioni dettagliate sulle modalità di configurazione di ESET Cluster tramite la procedura guidata, fare clic qui.

Per configurare ESET Cluster, sono disponibili due metodi di aggiunta dei nodi: in maniera automatica, attraverso l'utilizzo del cluster di failover Windows/cluster NLB esistente, o manualmente, attraverso la ricerca dei computer presenti in un gruppo di lavoro o dominio.

Rilevamento automatico: rileva automaticamente i nodi che sono già membri di un cluster di failover Windows/ cluster NLB e li aggiunge a ESET Cluster
Sfoglia: è possibile aggiungere manualmente i nodi digitando i nomi del server (membri dello stesso gruppo di lavoro o membri dello stesso dominio)

NOTA: non è necessario che i server siano membri di un cluster di failover Windows/cluster NLB per poter utilizzare la funzione ESET Cluster. Per l'utilizzo dei cluster ESET nel proprio ambiente di lavoro, non è necessario un cluster di failover Windows/cluster NLB.

Dopo aver aggiunto i nodi a ESET Cluster, è necessario installare ESET Mail Security su ciascuno di essi. Questa operazione viene eseguita automaticamente durante la configurazione di ESET Cluster.

Le credenziali richieste per l'installazione remota di ESET Mail Security su altri nodi cluster sono le seguenti:

- Scenario dominio: credenziali amministratore del dominio
- Scenario gruppo di lavoro: è necessario accertarsi che tutti i nodi utilizzino le stesse credenziali dell'account amministratore locale

In ESET Cluster è inoltre possibile utilizzare una combinazione di nodi aggiunti automaticamente come membri di un cluster di failover Windows/cluster NLB esistente e di nodi aggiunti manualmente (a condizione che si trovino nello stesso dominio).

i **NOTA:** non è possibile associare nodi del dominio a nodi del gruppo di lavoro.

Un altro requisito per l'utilizzo di ESET Cluster consiste nel fatto che l'opzione **Condivisione file e stampanti** sia attiva in Windows Firewall prima dell'avvio dell'installazione di ESET Mail Security sui nodi di ESET Cluster.

ESET Cluster può essere facilmente eliminato facendo clic su **Elimina cluster**. Ciascun nodo scriverà un record nel relativo rapporto eventi sull'ESET Cluster eliminato. Successivamente, tutte le regole del firewall ESET verranno rimosse da Windows Firewall. I primi nodi ritorneranno quindi nello stato precedente e potranno essere nuovamente utilizzati in un altro ESET Cluster, se necessario.

i **NOTA:** la creazione di ESET Cluster tra ESET Mail Security ed ESET File Security for Linux non è supportata.

In qualsiasi momento, è possibile aggiungere nuovi nodi a un ESET Cluster esistente eseguendo la **Procedura guidata cluster** in base alle modalità descritte in precedenza e qui.

Per ulteriori informazioni sulla configurazione di ESET Cluster, consultare la sezione Cluster di lavoro.

4.7.6 ESET Shell

eShell (abbreviazione di ESET Shell) è un'interfaccia della riga di comando per ESET Mail Security. Rappresenta un'alternativa all'interfaccia grafica utente (GUI). eShell offre tutte le funzionalità e le opzioni generalmente offerte dalla GUI. eShell consente di configurare e amministrare l'intero programma senza utilizzare la GUI.

In aggiunta a tutte le funzionalità disponibili nella GUI, offre anche l'opzione di utilizzo dell'automazione mediante l'esecuzione di script per poter configurare, modificare la configurazione o eseguire un'azione. eShell può inoltre risultare utile per gli utenti che preferiscono utilizzare la riga di comando rispetto alla GUI.

eShell può essere eseguito in due modalità:

- Modalità interattiva: risulta utile quando si desidera utilizzare eShell (non eseguire semplicemente un singolo comando) per attività quali la modifica della configurazione, la visualizzazione dei rapporti e così via. La modalità interattiva può essere utilizzata anche se ancora non si è familiarizzato con tutti i comandi. La modalità interattiva consente lo spostamento all'interno di eShell. Vengono inoltre visualizzati i comandi disponibili che è possibile utilizzare all'interno di un particolare contesto.

- Singolo comando/modalità batch: questa modalità può essere utilizzata se è necessario eseguire solo un comando senza accedere alla modalità interattiva di eShell. Questa operazione può essere eseguita dal prompt dei comandi di Windows digitando `eshell` con i comandi appropriati. Ad esempio:

```
eshell get status
```

oppure

```
eshell set antivirus status disabled
```

Per eseguire alcuni comandi (come nel secondo esempio indicato in precedenza) in modalità batch/script, sono disponibili due impostazioni che è necessario dapprima configurare. In caso contrario, verrà visualizzato il messaggio **Accesso negato** per motivi di sicurezza.

i **NOTA**: per disporre della funzionalità completa, si consiglia di aprire eShell utilizzando **Esegui come amministratore**. Le stesse condizioni si applicano anche durante l'esecuzione di un singolo comando attraverso il prompt dei comandi di Windows (cmd). Aprire il cmd utilizzando **Esegui come amministratore**. Diversamente, non sarà possibile eseguire tutti i comandi. Ciò dipende dal fatto che l'apertura del cmd o di eShell attraverso l'utilizzo di un account diverso da quello di amministratore non consentirà all'utente di disporre di autorizzazioni sufficienti.

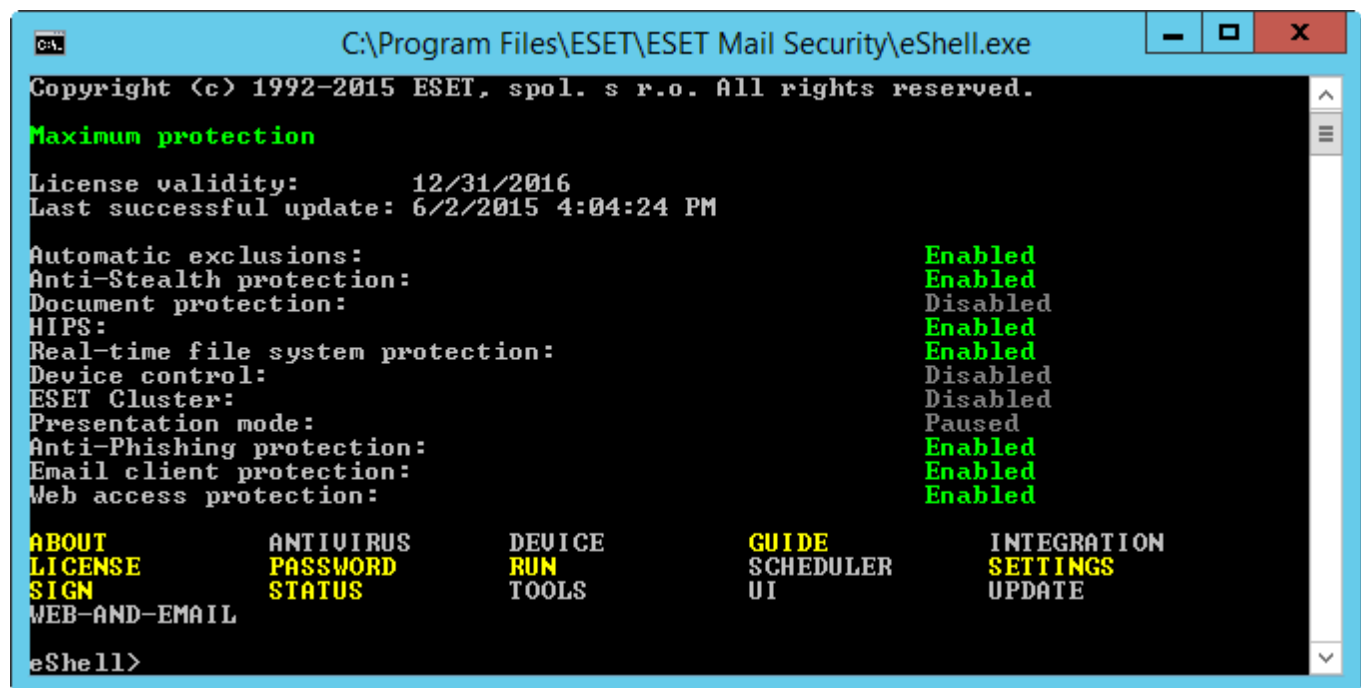
NOTA: per eseguire i comandi di eShell dal prompt dei comandi di Windows o i file batch, è necessario definire alcune impostazioni. Per ulteriori informazioni sull'esecuzione dei file batch, fare clic qui.

Per accedere alla modalità interattiva in eShell, è possibile utilizzare uno dei due metodi seguenti:

- Tramite il menu Start di Windows: **Start** > **Programmi** > **ESET** > **ESET File Security** > **ESET shell**
- Dal prompt dei comandi di Windows digitando `eshell` e premendo il tasto INVIO.

Quando si esegue per la prima volta eShell in modalità interattiva, viene visualizzata la schermata della prima esecuzione (guide).

NOTA: se si desidera visualizzare in futuro la schermata della prima esecuzione, digitare il comando `guide` . In questa schermata vengono visualizzati esempi di base su come utilizzare eShell con Sintassi, Prefisso, Percorso comando, Forme abbreviate, Alias e così via. Si tratta essenzialmente di una guida rapida all'utilizzo di eShell.

Alla successiva esecuzione di eShell, verrà visualizzata la seguente schermata:

NOTA: i comandi non fanno distinzione tra lettera maiuscola e minuscola ed è pertanto possibile eseguirli utilizzando entrambi i caratteri.

Personalizzare eShell

È possibile personalizzare eShell nel `contesto` ui eshell. È possibile configurare alias, colori, lingua e criterio di esecuzione per gli script, scegliere di visualizzare comandi nascosti e altre impostazioni.

4.7.6.1 Utilizzo

Sintassi

Per un corretto funzionamento, i comandi devono essere formattati nella sintassi corretta e devono essere composti da un prefisso, un contesto, argomenti, opzioni e così via. Di seguito viene riportata la sintassi generale utilizzata all'interno di eShell:

[<prefisso>] [<percorso comando>] <comando> [<argomenti>]

Esempio (verrà attivata la protezione del documento):
`SET ANTIVIRUS DOCUMENT STATUS ENABLED`

`SET` : un prefisso
`ANTIVIRUS DOCUMENT` : percorso a un particolare comando, un contesto al quale appartiene tale comando
`STATUS` : il comando stesso
`ENABLED` : un argomento per il comando

L'utilizzo di ? con argomento per il comando consente di visualizzare la sintassi di tale comando specifico. Ad esempio, STATUS ? consente di visualizzare la sintassi per il comando STATUS :

SINTASSI:

```
[get] | status
set status enabled | disabled
```

Si noti che [get] viene racchiuso tra parentesi quadre. Indica che il prefisso get è il prefisso predefinito per il comando status . Ciò significa che quando si esegue il comando status senza specificare un prefisso, verrà utilizzato in realtà il prefisso predefinito (in questo caso get status). L'utilizzo di comandi senza un prefisso consente di ridurre i tempi di digitazione. In genere get rappresenta il prefisso predefinito per la maggior parte dei comandi, ma è necessario accertarsi quale sia il prefisso predefinito per un determinato comando e che sia esattamente quello che si desidera eseguire.

NOTA: i comandi non fanno distinzione tra lettera maiuscola e minuscola per poter essere eseguiti.

Prefisso/operazione

Un prefisso rappresenta un'operazione. Il prefisso GET fornisce informazioni sulle modalità di configurazione di una determinata funzionalità di ESET Mail Security o consente di visualizzare lo stato, ad esempio GET ANTIVIRUS STATUS mostra lo stato di protezione corrente. Il prefisso SET consente di configurare la funzionalità o di modificarne lo stato (SET ANTIVIRUS STATUS ENABLED attiva la protezione).

Questi sono i prefissi che eShell consente di utilizzare. Un comando può o meno supportare uno dei seguenti prefissi:

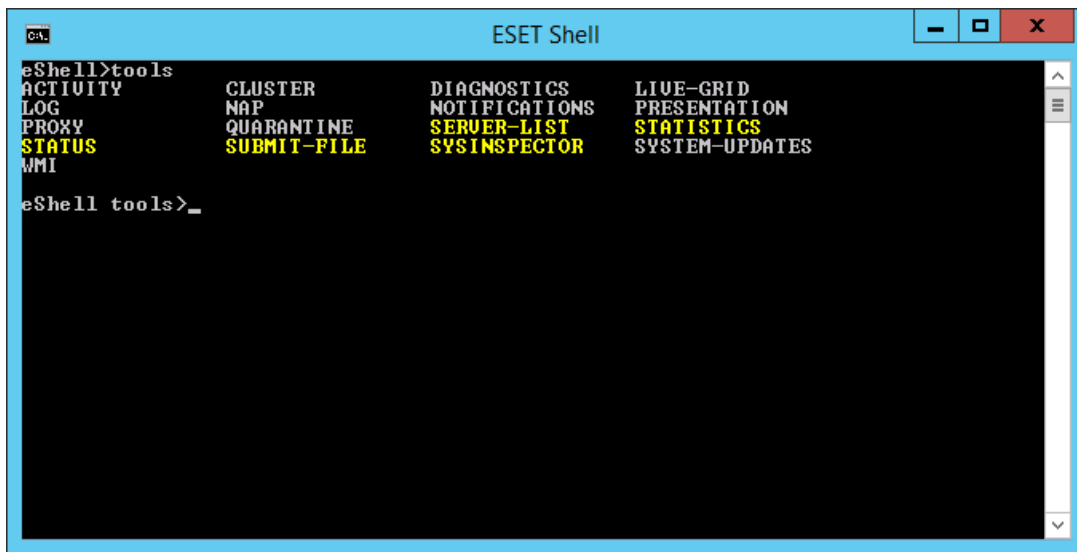
GET : ripristina impostazione/stato corrente
SET : configura valore/stato
SELECT : seleziona una voce
ADD : aggiunge una voce
REMOVE : rimuove una voce
CLEAR : rimuove tutti gli elementi/file
START : avvia un'azione
STOP : interrompe un'azione
PAUSE : sospende un'azione
RESUME : riprende un'azione
RESTORE : ripristina impostazioni predefinite/oggetto/file
SEND : invia un oggetto/file
IMPORT : importa da un file
EXPORT : esporta in un file

I prefissi quali GET e SET vengono utilizzati con numerosi comandi ma alcuni di essi (ad esempio EXIT) non utilizzano un prefisso.

Percorso del comando/contesto

I comandi sono posizionati in contesti che formano una struttura ad albero. Il livello superiore dell'albero è la radice. Quando si esegue eShell, si è al livello radice:

```
eShell>
```

È possibile eseguire un comando da tale posizione oppure immettere il nome del contesto per spostarsi all'interno della struttura ad albero. Ad esempio, quando si accede al contesto TOOLS, verranno elencati tutti i comandi e sottocontesti disponibili da questa posizione.

Le voci in giallo sono i comandi che è possibile eseguire, mentre quelle in grigio sono i sottocontesti ai quali è possibile accedere. Un sottocontesto contiene ulteriori comandi.

Se è necessario ritornare a un livello superiore, utilizzare .. (due punti). Ad esempio, se ci si trova nel contesto:

```
eShell antivirus startup>
```

digitare .. per passare a un livello superiore, ovvero a:

```
eShell antivirus>
```

Se si desidera ritornare alla radice da eShell antivirus startup> (che si trova a due livelli inferiori dalla radice), è sufficiente digitare .. .. (due punti e due punti separati da spazio). In questo modo, si passa a due livelli superiori che, in questo caso, corrispondono alla radice. Utilizzare la barra rovesciata \ per ritornare direttamente alla radice da un livello qualsiasi, indipendentemente dalla profondità di quello in cui ci si trova nella struttura dei contesti. Se si desidera ottenere un contesto particolare nei livelli superiori, basta semplicemente utilizzare il numero appropriato di .. necessario per raggiungere il livello desiderato. Utilizzare lo spazio come separatore. Ad esempio, se si desidera salire di tre livelli, utilizzare .. .. ..

Il percorso è relativo al contesto corrente. Se il comando è contenuto nel contesto corrente, non immettere un percorso. Ad esempio, per eseguire GET ANTIVIRUS STATUS immettere:

GET ANTIVIRUS STATUS : se ci si trova nel contesto radice (sulla riga di comando è visualizzato eShell>)
GET STATUS : se ci si trova nel contesto ANTIVIRUS (sulla riga di comando è visualizzato eShell antivirus>)
.. GET STATUS : se ci si trova nel contesto ANTIVIRUS STARTUP (sulla riga di comando è visualizzato eShell antivirus startup>)

NOTA: è possibile utilizzare un . singolo (punto) al posto di due .. in quanto il punto singolo è un abbreviazione dei due punti. Ad esempio:

. GET STATUS : se ci si trova nel contesto ANTIVIRUS STARTUP (sulla riga di comando è visualizzato eShell antivirus startup>)

Argomento
Un argomento è un'azione che viene eseguita per un particolare comando. Ad esempio, il comando CLEAN-LEVEL (posizionato in ANTIVIRUS REALTIME ENGINE) può essere utilizzato con i seguenti argomenti:

no - Nessuna pulizia
normal - Pulizia normale
strict : massima pulizia

Un altro esempio sono gli argomenti ENABLED oppure DISABLEDche vengono utilizzati per attivare o disattivare una determinata funzionalità.

Forma abbreviata/comandi abbreviati
eShell consente di abbreviare i contesti, i comandi e gli argomenti (a condizione che l'argomento sia un'opzione oppure un'opzione alternativa). Non è possibile abbreviare un prefisso o un argomento che sia un valore concreto, ad esempio un numero, un nome o un percorso.

Esempi della forma breve:

`set status enabled` => `set stat en`

`add antivirus common scanner-excludes C:\path\file.ext` => `add ant com scann C:\path\file.ext`

Nel caso in cui due comandi o contesti inizino con la stessa lettera, ad esempio `ABOUT` e `ANTIVIRUS` e si immette `A` come comando abbreviato, eShell non sarà in grado di scegliere quale comando dei due l'utente desidera eseguire. Verrà quindi visualizzato un messaggio di errore e verranno visualizzati i comandi che iniziano con la lettera "A" tra i quali scegliere:

```
eShell>a
Il seguente comando non è univoco: a

I seguenti comandi sono disponibili in questo contesto:
ABOUT: mostra informazioni sul programma
ANTIVIRUS - Modifiche apportate all'antivirus del contesto
```

Aggiungendo una o più lettere (ad esempio, `AB` anziché semplicemente `A`) eShell esegue il comando `ABOUT` poiché in questo caso risulta univoco.

NOTA: se si desidera essere certi che un comando venga eseguito come desiderato, si consiglia di non abbreviare i comandi, gli argomenti e così via e di utilizzare la forma completa. In questo modo, verrà eseguito esattamente come desiderato e si eviteranno errori indesiderati. Ciò è particolarmente utile nel caso dei file batch/script.

Completamento automatico
Si tratta di una nuova funzione di eShell prevista a partire dalla versione 2.0, molto simile al completamento automatico nel prompt dei comandi di Windows. Mentre il prompt dei comandi di Windows completa i percorsi dei file, eShell completa anche il comando, il contesto e i nomi delle operazioni. Il completamento dell'argomento non è supportato. Durante la digitazione del comando, premere semplicemente il tasto TAB (tabulazione) per completare o scorrere le variazioni disponibili. Premere MAIUSC + TAB per tornare indietro. L'utilizzo contestuale di forme abbreviate e del completamento automatico non è supportato. È infatti possibile utilizzare solo una funzione alla volta. Ad esempio, digitando `antivir real scan`, la pressione del tasto TAB non avrà alcun effetto. Digitare invece `antivir` e premere TAB per completare `antivirus`, continuare a digitare real + TAB e scan + TAB. È quindi possibile scorrere tutte le variazioni disponibili: scan-create, scan-execute, scan-open, ecc.

Alias
Un alias è un nome alternativo che può essere utilizzato per eseguire un comando, a condizione che al comando sia assegnato un alias. Sono disponibili alcuni alias predefiniti:

`(global) close` : esci
`(global) quit` : esci
`(global) bye` : esci
`warnlog` : eventi rapporto strumenti
`virlog` : rilevamenti rapporto strumenti
`antivirus on-demand log` : controlli del rapporto strumenti

"(global)" indica che il comando può essere utilizzato ovunque, indipendentemente dal contesto corrente. A un comando possono essere assegnati più alias. Ad esempio al comando `EXIT` è assegnato l'alias `CLOSE`, `QUIT` e `BYE`. Per uscire da eShell, è possibile utilizzare il comando `EXIT` oppure uno qualsiasi dei rispettivi alias. L'alias `VIRLOG` è per il comando `DETECTIONS` posizionato nel contesto `TOOLS` LOG. In questo modo, il comando Detections è disponibile dal contesto `ROOT` facilitando l'accesso (non è infatti necessario accedere a `TOOLS`, quindi al contesto `LOG` ed eseguirlo direttamente da `ROOT`).

eShell consente di definire alias personali. Comando `ALIAS` è disponibile nel `contesto` UI ESHELL.

Impostazioni protette con password
È possibile proteggere le impostazioni di ESET Mail Security con password. È possibile impostare la password

utilizzando la GUI o eShell utilizzando `il comando set ui access` lock-password. A questo punto, è necessario inserire la password in modo interattivo per alcuni comandi (come quelli che consentono di modificare le impostazioni o i dati). Se si desidera lavorare con eShell per un periodo di tempo più prolungato senza inserire ripetutamente la password, è possibile impostarne la memorizzazione in eShell utilizzando il comando `set` password. A questo punto, la password verrà compilata automaticamente per ciascun comando eseguito che la richiede. La password viene memorizzata fino all'uscita dell'utente da eShell. Ciò significa che sarà nuovamente necessario utilizzare il comando `set password` all'avvio della nuova sessione e se si desidera che eShell memorizzi la password.

Guide / Help
Quando si esegue il comando `GUIDE`, oppure `HELP` verrà visualizzata una schermata "della prima esecuzione" in cui viene illustrato come utilizzare eShell. Questo comando è disponibile nel contesto `ROOT` (`eShell>`).

Cronologia dei comandi
eShell conserva la cronologia dei comandi eseguiti in precedenza. Ciò è applicabile solo alla sessione eShell interattiva corrente. Quando si esce da eShell, la cronologia dei comandi non sarà più disponibile. Utilizzare i tasti freccia Su e Giù sulla tastiera per spostarsi all'interno della cronologia. Dopo aver trovato il comando desiderato, è possibile eseguirlo nuovamente o modificarlo senza doverlo digitare nuovamente dall'inizio.

CLS/Cancella schermata
Il comando `CLS` può essere utilizzato per cancellare la schermata. Funziona allo stesso modo del prompt dei comandi di Windows o delle interfacce della riga di comando simili.

EXIT/CLOSE/QUIT/BYE
Per chiudere o uscire da eShell, è possibile utilizzare uno di questi comandi (`EXIT`, `CLOSE`, `QUIT` oppure `BYE`).

4.7.6.2 Comandi

In questa sezione sono elencati alcuni comandi eShell di base con una descrizione a titolo di esempio.

i **NOTA**: i comandi non fanno distinzione tra lettera maiuscola e minuscola per poter essere eseguiti.

Esempi di comandi (contenuti nel contesto ROOT):

ABOUT

Mostra informazioni sul programma. Viene visualizzato il nome del prodotto installato, il numero di versione, i componenti installati, compreso il numero di versione di ciascun componente, e le informazioni di base sul server e il sistema operativo sul quale è in esecuzione ESET Mail Security.

PERCORSO CONTESTUALE:

```
radice
```

PASSWORD

In genere, per motivi di sicurezza, per eseguire comandi protetti con password, all'utente viene chiesto di immettere una password. Ciò è applicabile a comandi che disattivano la protezione antivirus o che potrebbero influenzare la funzionalità di ESET Mail Security. A ogni esecuzione di tale comando, all'utente verrà chiesto di inserire la password. Per evitare di doverla inserire ogni volta, l'utente può definire la password, che verrà ricordata da eShell e utilizzata automaticamente a ogni esecuzione di un comando protetto con password. Ciò significa che non sarà necessario inserire ogni volta la password.

i **NOTA**: la password impostata è valida solo per la sessione eShell interattiva corrente. Quando si esce da eShell, la password impostata non sarà più valida. Al successivo avvio di eShell, sarà necessario definirla nuovamente.

L'impostazione della password risulta inoltre molto utile anche quando si eseguono file batch/script. Di seguito viene riportato un esempio di file batch:

```
eshell start batch "&" set password plain <yourpassword> "&" set status disabled
```

Il precedente comando concatenato avvia una modalità batch, definisce una password che verrà utilizzata e disattiva la protezione.

PERCORSO CONTESTUALE:

`radice`

SINTASSI:

`[get] | restore password`

`set password [plain <password>]`

OPERAZIONI:

`get` : mostra la password

`set` : imposta o cancella la password

`restore` : cancella la password

ARGOMENTI:

`plain` : opzione per immettere la password come parametro

`password` : password

ESEMPI:

`set password plain <yourpassword>` : imposta una password che verrà utilizzata per i comandi protetti con password

`restore password` : cancella la password

ESEMPI:

`get password` : utilizzare questo comando per visualizzare se la password è configurata o meno (verranno visualizzati solo asterischi "*" e non la password stessa). Se non sono visibili asterischi, significa che la password non è impostata

`set password plain <yourpassword>` : utilizzare questo comando per impostare una password definita

`restore password` : questo comando cancella la password definita

STATUS

Fornisce informazioni relative allo stato di protezione corrente di ESET Mail Security (simile all'interfaccia utente).

PERCORSO CONTESTUALE:

`radice`

SINTASSI:

`[get] | restore status`

`set status disabled | enabled`

OPERAZIONI:

`get` : mostra lo stato della protezione antivirus

`set` : disattiva/attiva la protezione antivirus

`restore` : ripristina le impostazioni predefinite

ARGOMENTI:

`disabled` : disattiva la protezione antivirus

`enabled` : attiva la protezione antivirus

ESEMPI:

`get status` : mostra lo stato di protezione corrente

`set status disabled` : disattiva la protezione

`restore status` : ripristina l'impostazione predefinita della protezione (Attivata)

VIRLOG

Alias del comando `DETECTIONS` . Risulta utile per visualizzare le informazioni sulle infiltrazioni rilevate.

WARNLOG

Alias del comando `EVENTS` . Risulta utile per visualizzare le informazioni su vari eventi.

4.7.6.3 File batch/scripting

È possibile utilizzare eShell come utile strumento di scripting per l'automazione. Per utilizzare il file batch con eShell, crearne uno con un eShell e l'esecuzione interna di un comando. Ad esempio:

```
eshell get antivirus status
```

È inoltre possibile collegare i comandi. Tale operazione si rivela, ad esempio, necessaria se si desidera ottenere una particolare attività pianificata. Per far ciò, è necessario inserire il seguente comando:

```
eshell select scheduler task 4 "&" get scheduler action
```

La selezione di un oggetto (in questo caso, numero di attività 4) vale solitamente solo per un'istanza attualmente in esecuzione di eShell. In caso di esecuzione di questi due comandi uno di seguito all'altro, il secondo comando restituirebbe un errore del tipo "Nessuna attività selezionata o l'attività selezionata non è più esistente".

Per motivi di protezione, il criterio di esecuzione è impostato su "Scripting limitato" per impostazione predefinita. Ciò consente all'utente di utilizzare eShell come strumento di monitoraggio, ma non di apportare modifiche alla configurazione di ESET Mail Security. In caso di comandi che influiscono sulla sicurezza, come ad esempio la disattivazione della protezione, verrà visualizzato il messaggio **Accesso negato**. Per eseguire questi comandi in grado di modificare la configurazione, si consiglia di utilizzare file batch firmati.

Se, per un motivo specifico, è necessario modificare la configurazione mediante l'utilizzo di un singolo comando inserito manualmente nel prompt dei comandi di Windows, è necessario concedere l'accesso completo a eShell (scelta non consigliata). Per concedere l'accesso completo, utilizzare il comando `ui eshell shell-execution-policy` nella modalità interattiva di eShell stesso oppure tramite la GUI in **Configurazione avanzata** > **Interfaccia utente** > ESET Shell.

File batch firmati

eShell consente all'utente di proteggere i comuni file batch (*.bat) con una firma. Gli script vengono firmati con la stessa password utilizzata per la protezione delle impostazioni. Per firmare uno script, è necessario attivare dapprima la protezione delle impostazioni. È possibile eseguire questa operazione tramite la GUI oppure in eShell utilizzando il comando `set ui access` lock-password. Dopo aver configurato la password per la protezione delle impostazioni, è possibile iniziare a firmare i file batch.

Per firmare un file batch, eseguire `sign <script.bat>` dal contesto radice di eShell, dove *script.bat* è il percorso dello script che si desidera firmare. Inserire e confermare la password che verrà utilizzata per la firma. Questa password deve corrispondere a quella utilizzata per la protezione delle impostazioni. La firma viene posizionata in calce al file batch sotto forma di commento. Se lo script è stato precedentemente firmato, la nuova firma sostituirà quella esistente.

i **NOTA**: in caso di modifica del file batch precedentemente firmato, è necessario apporre nuovamente la firma.

i **NOTA**: se si modifica la password della protezione delle impostazioni, è necessario firmare nuovamente tutti gli script. In caso contrario, gli script non potranno essere eseguiti a causa della modifica della password per la protezione delle impostazioni. Ciò dipende dal fatto che la password inserita al momento della firma dello script deve corrispondere alla password per la protezione delle impostazioni sul sistema di destinazione.

Per eseguire il file batch firmato dal prompt dei comandi di Windows come attività pianificata, utilizzare il comando

seguente:

```
eshell run <script.bat>
```

Dove script.bat è il percorso del file batch. Ad esempio, `eshell run d:\myeshellscript.bat`

4.7.7 ESET SysInspector

ESET SysInspector è un'applicazione che esamina a fondo il computer, raccoglie informazioni dettagliate sui componenti del sistema, quali i driver e le applicazioni installati, le connessioni di rete o le voci di registro importanti e valuta il livello di rischio di ciascun componente. Tali informazioni possono risultare utili per determinare la causa di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

Nella finestra di dialogo ESET SysInspector sono visualizzate le seguenti informazioni sui rapporti creati:

- **Ora**: ora di creazione del rapporto.
- **Commento**: breve commento.
- **Utente**: nome dell'utente che ha creato il rapporto.
- **Stato**: stato di creazione del rapporto.

Sono disponibili le azioni seguenti:

- **Apri**: apre il rapporto creato. È inoltre possibile eseguire tale operazione facendo clic con il pulsante destro del mouse sul rapporto creato e selezionando **Mostra** dal menu contestuale.
- **Confronta**: consente di mettere a confronto due rapporti esistenti.
- **Crea**: crea un nuovo rapporto. Attendere il completamento del rapporto di ESET SysInspector (**Stato**: Creato).
- **Elimina**: rimuove dall'elenco i rapporti selezionati.

Fare clic con il pulsante destro del mouse su uno o più rapporti selezionati per visualizzare le opzioni seguenti del menu contestuale:

- **Mostra**: apre il rapporto selezionato in ESET SysInspector (funzione uguale a un doppio clic su un rapporto).
- **Crea**: crea un nuovo rapporto. Attendere il completamento del rapporto di ESET SysInspector (**Stato** visualizzato come Creato)
- **Elimina tutto**: consente di eliminare tutti i rapporti.
- **Esporta**: esporta il rapporto in un file *.xml* o in un file *.xml* compresso.

4.7.7.1 Crea uno snapshot dello stato del computer

Inserire un breve commento che descrive il rapporto da creare, quindi premere il pulsante **Aggiungi**. Attendere il completamento del rapporto di ESET SysInspector (Stato: Creato). La creazione del rapporto potrebbe richiedere alcuni minuti in base alla configurazione hardware e ai dati di sistema.

4.7.7.2 ESET SysInspector

4.7.7.2.1 Introduzione a ESET SysInspector

L'applicazione ESET SysInspector ispeziona il computer in modo approfondito e visualizza i dati raccolti in modo esauriente. La raccolta di informazioni su driver e applicazioni installati, connessioni di rete o importanti voci di registro semplifica il controllo di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

È possibile accedere a ESET SysInspector in due modi: dalla versione integrata nelle soluzioni ESET Security o scaricando gratuitamente la versione indipendente (SysInspector.exe) dal sito Web ESET. Le funzionalità e i comandi di entrambe le versioni sono identici. L'unica differenza consiste nella gestione dei risultati. La versione indipendente e quella integrata consentono entrambe di esportare snapshot del sistema su un file *XML* e salvarli su disco. La versione integrata consente tuttavia anche di memorizzare gli snapshot di sistema direttamente in **Strumenti** > **ESET SysInspector** (tranne ESET Remote Administrator).

È necessario attendere qualche minuto per consentire a ESET SysInspector di controllare il computer. A seconda

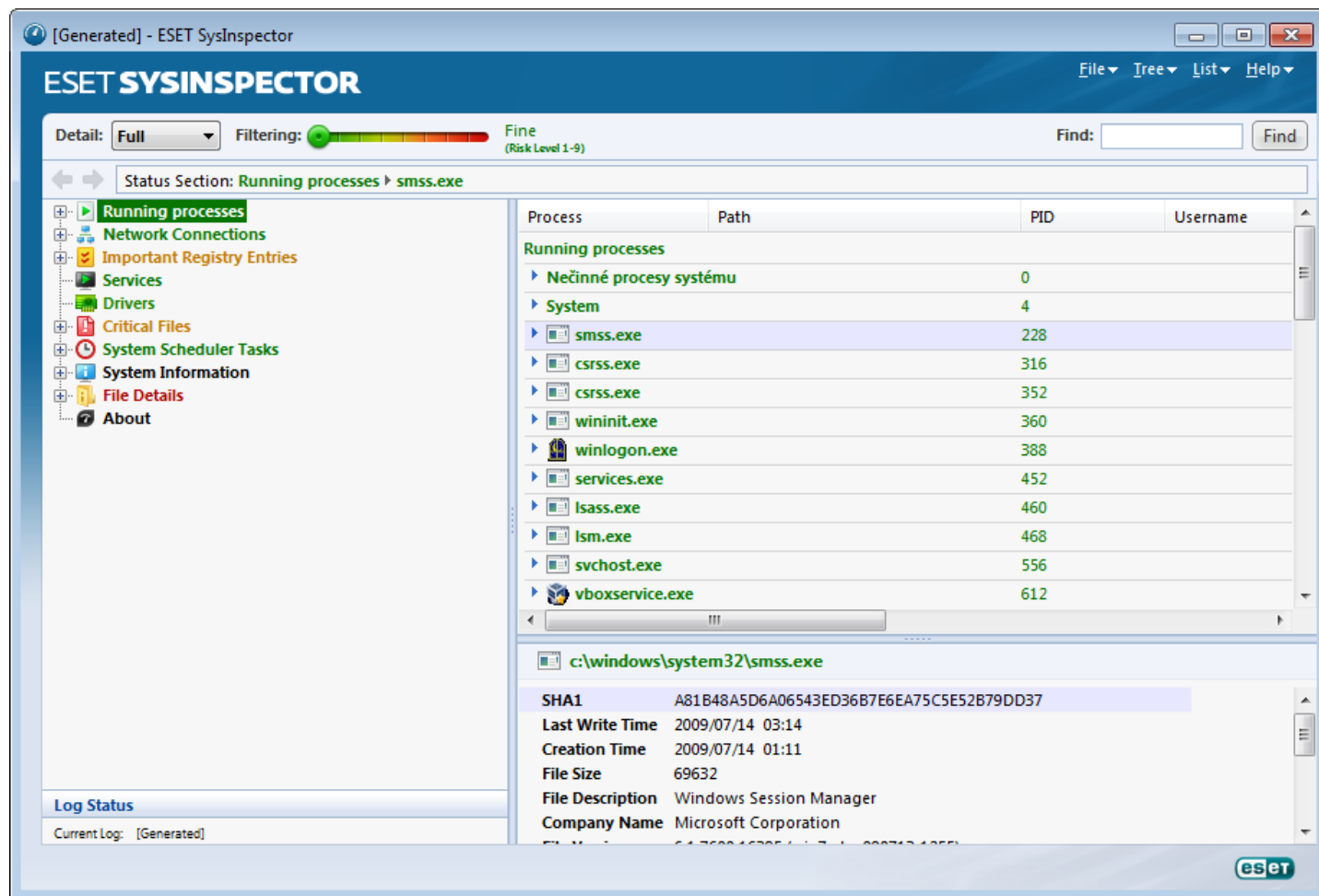
della configurazione hardware, del sistema operativo e del numero di applicazioni installate nel computer in uso, questa operazione potrebbe richiedere da 10 secondi ad alcuni minuti.

4.7.7.2.1.1 Avvio di ESET SysInspector

Per avviare ESET SysInspector è sufficiente eseguire il file eseguibile *SysInspector.exe* scaricato dal sito Web ESET.

È necessario attendere che l'applicazione abbia esaminato il sistema in uso. Questa operazione potrebbe richiedere diversi minuti a seconda dell'hardware e dei dati raccolti.

4.7.7.2.2 Interfaccia utente e utilizzo dell'applicazione

Per chiarezza, la finestra principale è stata divisa in quattro sezioni principali: i comandi del programma sono posizionati nella parte superiore della finestra; a sinistra viene visualizzata la finestra di spostamento, a destra, nella parte centrale, è disponibile la finestra Descrizione e, infine, nella parte inferiore destra della schermata viene visualizzata la finestra Dettagli. Nella sezione Stato rapporto sono elencati i parametri principali di un rapporto (filtro usato, tipo di filtro, se il rapporto è il risultato di un confronto e così via).

4.7.7.2.2.1 Comandi del programma

La presente sezione contiene la descrizione di tutti i comandi del programma disponibili in ESET SysInspector.

File

Selezionare **File** per memorizzare lo stato attuale del sistema per un'analisi futura oppure aprire un rapporto precedentemente archiviato. Ai fini della pubblicazione, è consigliabile generare un rapporto **Adatto per l'invio**. In questo formato, nel rapporto vengono omesse informazioni sensibili (nome utente attuale, nome computer, nome dominio, privilegi utente attuale, variabili d'ambiente e così via).

NOTA: è possibile aprire i rapporti di ESET SysInspector precedentemente archiviati trascinandoli nella finestra principale.

Struttura

Consente di espandere o chiudere tutti i nodi e di esportare le sezioni selezionate sullo script di servizio.

Elenco

Contiene funzioni per uno spostamento più pratico all'interno del programma e varie altre funzioni, ad esempio la ricerca di informazioni su Internet.

Guida

Contiene informazioni sull'applicazione e sulle relative funzioni.

Dettaglio

Questa impostazione influenza le informazioni visualizzate nella finestra principale al fine di semplificarne l'utilizzo. Nella modalità "Base" si ha accesso alle informazioni utilizzate per trovare soluzioni a problemi comuni del sistema. Nella modalità "Media" il programma visualizza i dettagli meno utilizzati, mentre nella modalità "Completa", ESET SysInspector mostra tutte le informazioni necessarie alla soluzione di problemi specifici.

Filtraggio elementi

Il filtraggio elementi viene utilizzato soprattutto per individuare file o voci di registro sospetti all'interno del sistema. Regolando il cursore, è possibile filtrare gli elementi in base al livello di rischio. Se il cursore si trova all'estrema sinistra (Livello di rischio 1) vengono visualizzati tutti gli elementi. Spostando il cursore a destra, il programma esclude tutti gli elementi meno rischiosi rispetto al livello di rischio attuale, visualizzando solo gli elementi che risultano più sospetti rispetto al livello visualizzato. Quando il cursore si trova all'estrema destra, il programma visualizza solo gli elementi dannosi conosciuti.

Tutti gli elementi contrassegnati con un livello di rischio compreso tra 6 e 9 rappresentano un rischio per la sicurezza. Se ESET SysInspector ha rilevato un elemento di questo tipo, si consiglia di eseguire il controllo del sistema con ESET Online Scanner, se non si utilizzano alcune delle soluzioni di protezione di ESET. ESET Online Scanner è un servizio gratuito.

NOTA: il Livello di rischio di un elemento può essere determinato rapidamente confrontandone il colore con quello del cursore Livello di rischio.

Cerca

L'opzione Cerca può essere utilizzata per individuare rapidamente un elemento specifico in base al nome o parte di esso. I risultati della richiesta di ricerca vengono visualizzati nella finestra Descrizione.

Ritorna

Facendo clic sulla freccia indietro o avanti è possibile tornare alle informazioni precedentemente visualizzate nella finestra Descrizione. Utilizzare i tasti Cancella e Barra spaziatrice anziché fare clic avanti e indietro all'interno del programma.

Sezione stato

Visualizza il nodo corrente nella finestra di spostamento.

Importante: gli elementi evidenziati in rosso sono sconosciuti. Per tale motivo, il programma li segna come potenzialmente pericolosi. Se un elemento è segnalato in rosso, non implica automaticamente che sia possibile eliminare il file. Prima di procedere all'eliminazione, assicurarsi che i file siano effettivamente pericolosi o non necessari.

4.7.7.2.2.2 Spostarsi all'interno di ESET SysInspector

ESET SysInspector divide vari tipi di informazioni in numerose sezioni di base, dette nodi. Se disponibili, ulteriori dettagli saranno visualizzabili espandendo ciascun nodo nei relativi sottonodi. Per espandere o comprimere un nodo, fare doppio clic sul nome del nodo o, in alternativa, selezionare ⊞ o ⊟ accanto al nome del nodo. Spostandosi nella struttura ad albero di nodi e sottonodi della finestra di spostamento, sono disponibili vari dettagli su ciascun nodo presente nella finestra Descrizione. Spostandosi tra gli elementi della finestra Descrizione, è possibile visualizzare ulteriori dettagli relativi a ciascun elemento nella finestra Dettagli.

Di seguito vengono riportate le descrizioni dei nodi principali presenti nella finestra di spostamento e le relative informazioni delle finestre Descrizione e Dettagli.

Processi in esecuzione

Questo nodo contiene informazioni sulle applicazioni e sui processi in esecuzione durante la generazione del rapporto. Nella finestra Descrizione sono disponibili dettagli aggiuntivi su ciascun processo, ad esempio le librerie dinamiche utilizzate dal processo e la loro posizione nel sistema, il nome del produttore dell'applicazione e il livello di rischio del file.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

NOTA: un sistema operativo è basato su diversi componenti kernel, in esecuzione 24 ore su 24, 7 giorni su 7, che forniscono funzioni fondamentali e di base per le altre applicazioni utente. In alcuni casi, tali processi sono visualizzati nello strumento ESET SysInspector con il percorso file preceduto da \??\. Quei simboli forniscono un'ottimizzazione per i processi in questione prima di avviarli e risultano sicuri per il sistema.

Connessioni di rete

La finestra Descrizione contiene un elenco di processi e applicazioni che comunicano sulla rete utilizzando il protocollo selezionato nella finestra di spostamento (TCP o UDP), unitamente all'indirizzo remoto a cui è collegata l'applicazione. È inoltre possibile verificare gli indirizzi IP dei server DNS.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

Voci importanti del Registro di sistema

Contiene un elenco delle voci di registro selezionate che sono spesso correlate a vari problemi del sistema, ad esempio quelle che indicano i programmi di avvio, oggetti browser helper (BHO) e così via.

Nella finestra Descrizione è possibile visualizzare i file correlati a voci di registro specifiche. Nella finestra Dettagli è possibile visualizzare maggiori informazioni.

Servizi

La finestra Descrizione contiene un elenco di file registrati come Servizi Windows. Nella finestra Dettagli è possibile controllare il modo in cui è impostato l'avvio del servizio insieme ai dettagli specifici del file.

Driver

Un elenco di driver installati nel sistema.

File critici

Nella finestra Descrizione è visualizzato il contenuto dei file critici relativi al sistema operativo Microsoft Windows.

Attività di pianificazione di sistema

Contiene un elenco delle attività avviate dall'Utilità di pianificazione di Windows a un orario/intervallo specificato.

Informazioni di sistema

Contiene informazioni dettagliate sull'hardware e sul software, oltre a informazioni sulle variabili d'ambiente

impostate, sui diritti utente e sui rapporti eventi di sistema.

Dettagli file

Un elenco di file di sistema importanti e di file presenti nella cartella Programmi. Per maggiori informazioni sui file in questione, fare riferimento alle finestre Descrizione e Dettagli.

Informazioni su

Informazioni sulla versione di ESET SysInspector ed elenco dei moduli del programma.

I tasti di scelta rapida che possono essere utilizzati con ESET SysInspector includono:

File

Ctrl+O	apre il rapporto esistente
Ctrl+S	salva i rapporti creati

Genera

Ctrl+G	genera uno snapshot di stato computer standard
Ctrl+H	genera uno snapshot di stato computer che potrebbe registrare anche informazioni sensibili

Filtraggio elementi

1, O	non a rischio, visualizzati gli elementi con livello di rischio 1-9
2	non a rischio, visualizzati gli elementi con livello di rischio 2-9
3	non a rischio, visualizzati gli elementi con livello di rischio 3-9
4, U	sconosciuto, visualizzati gli elementi con livello di rischio 4-9
5	sconosciuto, visualizzati gli elementi con livello di rischio 5-9
6	sconosciuto, visualizzati gli elementi con livello di rischio 6-9
7, B	a rischio, visualizzati gli elementi con livello di rischio 7-9
8	a rischio, visualizzati gli elementi con livello di rischio 8-9
9	a rischio, visualizzati gli elementi con livello di rischio 9
-	diminuisce il livello di rischio
+	aumenta il livello di rischio
Ctrl+9	modalità di filtraggio, livello uguale o più alto
Ctrl+0	modalità di filtraggio, solo livello uguale

Visualizza

Ctrl+5	visualizza per fornitore, tutti i fornitori
Ctrl+6	visualizza per fornitore, solo Microsoft
Ctrl+7	visualizza per fornitore, tutti gli altri fornitori
Ctrl+3	mostra tutti i dettagli
Ctrl+2	livello di dettaglio medio
Ctrl+1	visualizzazione di base
Cancella	indietro di un passaggio
Barra spaziatrice	avanti di un passaggio
Ctrl+W	espande la struttura
Ctrl+Q	comprime la struttura

Altri comandi

Ctrl+T	va alla posizione originale dell'elemento dopo averlo selezionato nei risultati di ricerca
Ctrl+P	visualizza informazioni di base su un elemento
Ctrl+A	visualizza informazioni complete su un elemento
Ctrl+C	copia la struttura dell'elemento corrente
Ctrl+X	copia gli elementi
Ctrl+B	trova su Internet le informazioni sui file selezionati
Ctrl+L	apre la cartella dove si trova il file selezionato

Ctrl+R	apre la voce corrispondente nell'editor del Registro di sistema
Ctrl+Z	copia un percorso di un file (se l'elemento è relativo a un file)
Ctrl+F	passa al campo di ricerca
Ctrl+D	chiude i risultati di ricerca
Ctrl+E	esegue lo script di servizio

Confronto

Ctrl+Alt+O	apre il rapporto originale/comparativo
Ctrl+Alt+R	annulla il confronto
Ctrl+Alt+1	visualizza tutti gli elementi
Ctrl+Alt+2	visualizza solo gli elementi aggiunti, il rapporto mostrerà gli elementi presenti nel rapporto corrente
Ctrl+Alt+3	visualizza solo gli elementi rimossi, il rapporto mostrerà gli elementi presenti nel rapporto precedente
Ctrl+Alt+4	visualizza solo gli elementi sostituiti (compresi i file)
Ctrl+Alt+5	visualizza solo le differenze tra i rapporti
Ctrl+Alt+C	visualizza il confronto
Ctrl+Alt+N	visualizza il rapporto corrente
Ctrl+Alt+P	apre il rapporto precedente

Varie

F1	visualizza la guida
Alt+F4	chiude il programma
Alt+Maiusc+F4	chiude il programma senza chiedere
Ctrl+I	statistiche rapporto

4.7.7.2.2.3 Confronta

La funzione Confronta consente di mettere a confronto due rapporti esistenti. Il risultato di questa funzione è una serie di elementi non comuni ai due rapporti. È la soluzione adatta se si desidera rilevare le modifiche nel sistema ed è un utile strumento per individuare l'attività del codice dannoso.

Dopo l'avvio, l'applicazione crea un nuovo rapporto, visualizzato in una nuova finestra. Andare a **File** > **Salva rapporto** per salvare un rapporto in un file. I file di rapporto possono essere aperti e visualizzati in un secondo momento. Per aprire un rapporto esistente, accedere a **File** > **Apri rapporto**. Nella finestra principale del programma, ESET SysInspector visualizza sempre un rapporto alla volta.

Il confronto tra due rapporti offre il vantaggio di visualizzare un rapporto attualmente attivo e uno salvato in un file. Per confrontare due rapporti, utilizzare l'opzione **File** > **Confronta rapporto** e scegliere **Seleziona file**. Il rapporto selezionato verrà confrontato con quello attivo nelle finestre principali del programma. Nel rapporto comparativo saranno visualizzate solo le differenze tra i due.

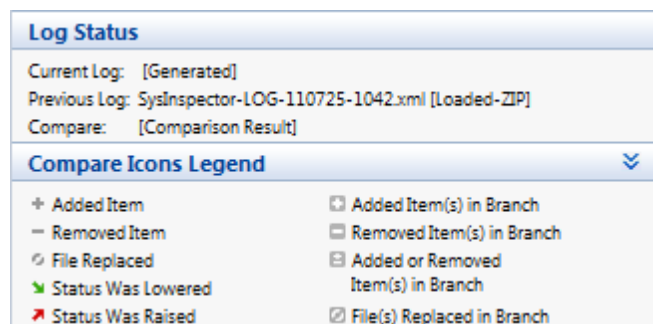
NOTA: se si mettono a confronto due file di rapporto, selezionando **File** > **Salva rapporto** e salvandoli in un file ZIP, verranno salvati entrambi i file. Se si apre il file in un secondo momento, i rapporti contenuti verranno automaticamente messi a confronto.

Accanto agli elementi visualizzati, ESET SysInspector mostra i simboli che identificano le differenze tra i rapporti confrontati.

Gli elementi contrassegnati con - si trovano solo nel rapporto attivo e non erano presenti nel rapporto comparativo aperto. Gli elementi contrassegnati con + erano presenti solo nel rapporto aperto e non sono presenti in quello attivo.

Descrizione di tutti i simboli che possono essere visualizzati accanto agli elementi:

- nuovo valore, non presente nel rapporto precedente
- la sezione della struttura contiene nuovi valori
- valore rimosso, presente solo nel rapporto precedente
- la sezione della struttura contiene i valori rimossi
- il valore/file è stato modificato
- la sezione della struttura contiene valori/file modificati
- il livello di rischio è diminuito/era più alto nel precedente rapporto
- il livello di rischio è aumentato/era più basso nel precedente rapporto

Nella sezione relativa alla descrizione visualizzata nell'angolo in basso a sinistra vengono descritti tutti i simboli e mostrati i nomi dei rapporti messi a confronto.

Qualsiasi rapporto comparativo può essere salvato in un file e aperto successivamente.

Esempio

Generare e salvare un rapporto, registrando le informazioni originali sul sistema, in un file denominato previous.xml. Dopo aver apportato le modifiche al sistema, aprire ESET SysInspector e attendere che venga generato un nuovo rapporto. Salvarlo in un file denominato *current.xml*.

Al fine di rilevare le modifiche tra i due rapporti, andare a **File** > **Confronta rapporti**. Il programma crea un rapporto comparativo che visualizza le differenze tra i due.

È possibile ottenere lo stesso risultato utilizzando la seguente opzione della riga di comando:

SysIsnpector.exe current.xml previous.xml

4.7.7.2.3 Parametri della riga di comando

ESET SysInspector supporta la generazione di rapporti dalla riga di comando con i seguenti parametri:

/gen	genera un rapporto direttamente dalla riga di comando senza eseguire l'interfaccia utente
/privacy	genera un rapporto escludendo informazioni sensibili
/zip	archivia il rapporto risultante direttamente sul disco in un file compresso
/silent	nasconde la barra di avanzamento della generazione del rapporto
/help, /?	visualizza informazioni sui parametri della riga di comando

Esempi

Per caricare un rapporto specifico direttamente nel browser, digitare: *SysInspector.exe "c:\clientlog.xml"*
Per generare un rapporto in un percorso corrente, digitare: *SysInspector.exe /gen*
Per generare un rapporto in una cartella specifica, digitare: *SysInspector.exe /gen="c:\folder\"*
Per generare un rapporto in un file/percorso specifico, digitare: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*
Per generare un rapporto escludendo le informazioni sensibili direttamente in un file compresso, digitare: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*
Per confrontare due rapporti, digitare: *SysInspector.exe "current.xml" "original.xml"*

NOTA: se il nome di un file/cartella contiene uno spazio vuoto, è necessario inserirlo tra virgolette.

4.7.7.2.4 Script di servizio

Lo script di servizio è uno strumento utile per i clienti che utilizzano ESET SysInspector in quanto consente di rimuovere facilmente gli oggetti indesiderati dal sistema.

Lo script di servizio consente all'utente di esportare l'intero rapporto di ESET SysInspector o le parti selezionate. Al termine dell'esportazione, è possibile selezionare gli oggetti indesiderati da eliminare. È quindi possibile eseguire il rapporto modificato per eliminare gli oggetti contrassegnati.

Lo script di servizio è adatto agli utenti avanzati che hanno già acquisito esperienza nella diagnostica dei problemi del sistema. Le modifiche effettuate da persone non qualificate potrebbero causare danni al sistema operativo.

Esempio

Se si sospetta che il computer sia infettato da un virus non rilevato dal programma antivirus, attenersi alle seguenti istruzioni dettagliate:

- Eseguire ESET SysInspector per generare un nuovo snapshot del sistema.
- Selezionare il primo elemento della sezione a sinistra (nella struttura ad albero), premere Ctrl ed evidenziare l'ultimo elemento per selezionarli tutti.
- Fare clic con il pulsante destro del mouse sugli oggetti selezionati e scegliere l'opzione del menu contestuale **Esporta sezioni selezionate a script di servizio**.
- Gli oggetti selezionati verranno esportati in un nuovo rapporto.
- Questo è il passaggio più importante dell'intera procedura: aprire il nuovo rapporto e cambiare l'attributo - in + per tutti gli oggetti che si desidera rimuovere. Fare attenzione a non contrassegnare file/oggetti importanti del sistema operativo.
- Aprire ESET SysInspector, fare clic su **File** > **Esegui script di servizio** e immettere il percorso dello script.
- Fare clic su **OK** per eseguire lo script.

4.7.7.2.4.1 Generazione dello script di servizio

Per generare uno script, fare clic con il pulsante destro del mouse su qualsiasi voce della struttura del menu (nel riquadro a sinistra) nella finestra principale di ESET SysInspector. Selezionare l'opzione **Esporta tutte le sezioni a script di servizio** o l'opzione **Esporta sezioni selezionate a script di servizio** nel menu contestuale.

NOTA: non è possibile esportare lo script di servizio quando vengono confrontati due rapporti.

4.7.7.2.4.2 Struttura dello script di servizio

Nella prima riga dell'intestazione dello script sono disponibili informazioni sulla versione del motore (ev), sulla versione dell'interfaccia utente (gv) e sulla versione del rapporto (lv). Questi dati possono essere utilizzati per tenere traccia delle possibili variazioni nel file XML che genera lo script e prevenire eventuali incoerenze durante l'esecuzione. Non modificare questa parte dello script.

La restante parte del file è suddivisa in sezioni in cui è possibile modificare gli elementi (indicare quelli che saranno elaborati dallo script). È possibile contrassegnare gli elementi da elaborare sostituendo il carattere "-" davanti a un elemento con il carattere "+". Le sezioni dello script sono separate tra loro mediante una riga vuota. A ogni sezione viene assegnato un numero e un titolo.

01) Processi in esecuzione

Questa sezione contiene un elenco di tutti i processi in esecuzione nel sistema. Ogni processo è identificato mediante il proprio percorso UNC e, successivamente, dal rispettivo codice hash CRC16 tra asterischi (*).

Esempio:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Nell'esempio, è stato selezionato un processo, module32.exe (contrassegnato dal carattere "+"). Il processo

terminerà all'esecuzione dello script.

02) Moduli caricati

In questa sezione sono contenuti i moduli di sistema attualmente in uso.

Esempio:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Nell'esempio, il modulo khbekhb.dll è stato contrassegnato con "+". All'esecuzione dello script, i processi che eseguono tale modulo specifico verranno riconosciuti e interrotti.

03) Connessioni TCP

Questa sezione contiene informazioni sulle connessioni TCP esistenti.

Esempio:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

All'esecuzione dello script, verrà individuato il proprietario del socket nelle connessioni TCP contrassegnate e il socket verrà interrotto, liberando le risorse del sistema.

04) Endpoint UDP

Questa sezione contiene informazioni sugli endpoint UDP esistenti.

Esempio:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

All'esecuzione dello script, verrà isolato il proprietario del socket sugli endpoint UDP contrassegnati e il socket verrà interrotto.

05) Voci server DNS

Questa sezione contiene informazioni sulla configurazione del server DNS corrente.

Esempio:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

All'esecuzione dello script, le voci del server DNS contrassegnate verranno rimosse.

06) Voci importanti del Registro di sistema

Questa sezione contiene informazioni su importanti voci del Registro di sistema.

Esempio:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

All'esecuzione dello script, le voci contrassegnate verranno eliminate, ridotte a valori a 0 byte o ripristinate sui valori predefiniti. L'azione da eseguire su una particolare voce dipende dalla categoria della voce stessa e dal valore principale nel Registro di sistema specifico.

07) Servizi

In questa sezione sono riportati i servizi registrati all'interno del sistema.

Esempio:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

All'esecuzione dello script, i servizi contrassegnati e i relativi servizi dipendenti verranno interrotti e disinstallati.

08) Driver

In questa sezione sono riportati i driver installati.

Esempio:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Quando si esegue lo script, i driver selezionati verranno arrestati. Tenere presente che alcuni driver non possono essere arrestati.

09) File critici

Questa sezione contiene informazioni sui file critici per il sistema operativo.

Esempio:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Gli elementi selezionati saranno eliminati o ripristinati sui valori originali.

4.7.7.2.4.3 Esecuzione degli script di servizio

Contrassegnare tutti gli elementi desiderati, quindi salvare e chiudere lo script. Eseguire lo script modificato direttamente dalla finestra principale di ESET SysInspector selezionando l'opzione **Esegui script di servizio** dal menu File. All'apertura di uno script, verrà visualizzato il seguente messaggio: **Eseguire lo script di servizio "%Scriptname %"?** Dopo aver confermato, verrà visualizzato un altro messaggio per segnalare che lo script di servizio che si sta cercando di eseguire non è stato firmato. Fare clic su **Esegui** per avviare lo script.

Verrà visualizzata una finestra di dialogo per confermare la corretta esecuzione dello script.

Se lo script è stato eseguito solo parzialmente, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio è stato eseguito parzialmente. Visualizzare il rapporto degli errori?** Selezionare **Sì** per visualizzare un rapporto completo degli errori in cui sono indicate le operazioni non eseguite.

Se lo script non viene riconosciuto, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio selezionato non è firmato. L'esecuzione di script sconosciuti o non firmati potrebbe causare seri danni ai dati nel computer. Eseguire lo script e le azioni?** Ciò potrebbe essere causato da incoerenze all'interno dello script (intestazione danneggiata, titolo della sezione danneggiato, linea vuota tra le sezioni e così via). È possibile riaprire il file di script e correggere gli errori all'interno dello script o creare un nuovo script di servizio.

4.7.7.2.5 Domande frequenti

ESET SysInspector richiede privilegi di amministratore per l'esecuzione?

Anche se per eseguire ESET SysInspector non sono necessari privilegi di amministratore, alcune informazioni raccolte possono essere visualizzate solo da un account amministratore. Eseguendo il programma come utente standard o utente con restrizioni, si raccoglieranno meno informazioni sull'ambiente operativo in uso.

ESET SysInspector crea un file di rapporto?

ESET SysInspector può creare un file di rapporto relativo alla configurazione del computer in uso. Per salvarlo, selezionare **File** > **Salva rapporto** dal menu principale. I rapporti vengono salvati nel formato XML. Per impostazione predefinita, i file vengono salvati nella directory *%USERPROFILE%\Documenti*\, con una convenzione di denominazione file "SysInpsector-%COMPUTERNAME%-AAMMGG-HHMM.XML". Se preferibile, è possibile modificare la posizione e il nome del file di rapporto prima di salvarlo.

Come si visualizza il file di rapporto di ESET SysInspector?

Per visualizzare un file di rapporto creato da ESET SysInspector, eseguire il programma e selezionare **File** > **Apri rapporto** dal menu principale. È anche possibile trascinare i file di rapporto all'interno dell'applicazione ESET SysInspector. Se è necessario consultare frequentemente i file di rapporto di ESET SysInspector, è consigliabile creare un collegamento sul Desktop al file SYSINSPECTOR.EXE. Sarà quindi sufficiente trascinare i file di rapporto sopra di esso per poterli visualizzare. Per motivi di protezione, in Windows Vista/7 la funzione di trascinamento della selezione tra finestre con differenti autorizzazioni di protezione potrebbe non essere disponibile.

È disponibile una specifica per il formato del file di rapporto? E per quanto riguarda un SDK?

Attualmente non è disponibile né una specifica per il file di rapporto né un SDK, in quanto il programma è ancora in fase di sviluppo. Dopo il rilascio del programma, potrebbero essere forniti sulla base dei commenti e delle richieste dei clienti.

In che modo ESET SysInspector valuta il rischio di un determinato oggetto?

Nella maggior parte dei casi, ESET SysInspector assegna livelli di rischio agli oggetti (file, processi, chiavi di registro e così via), utilizzando una serie di regole euristiche che esaminano le caratteristiche di ciascun oggetto e ne valutano quindi le potenzialità come attività dannosa. Sulla base di tali euristiche, agli oggetti viene assegnato un livello di rischio da 1 - Non a rischio (verde) a 9 - A rischio (rosso). Nel riquadro di spostamento a sinistra, le sezioni sono colorate sulla base del livello di rischio più elevato di un oggetto al loro interno.

Un livello di rischio "6 - Sconosciuto (rosso)" significa che un oggetto è pericoloso?

Le valutazioni di ESET SysInspector non garantiscono che un oggetto sia dannoso. Questa affermazione dovrebbe essere eseguita da un esperto di sicurezza. ESET SysInspector è progettato per fornire una rapida valutazione agli esperti di sicurezza, in modo da informarli su quali oggetti del sistema potrebbero richiedere una loro ulteriore analisi in presenza di comportamento anomalo.

Perché ESET SysInspector si collega a Internet quando viene avviato?

Al pari di molte applicazioni, ESET SysInspector è provvisto di firma digitale, un certificato che garantisce la pubblicazione del software da parte di ESET e l'assenza di alterazione dello stesso. Al fine di verificare il certificato, il sistema operativo contatta un'autorità di certificazione per verificare l'identità dell'autore del software. Si tratta di una procedura comune eseguita su tutti i programmi con firma digitale eseguiti in Microsoft Windows.

Cos'è la tecnologia Anti-Stealth?

La tecnologia Anti-Stealth assicura un efficace rilevamento dei rootkit.

Se il sistema viene attaccato da codice dannoso che si comporta come un rootkit, l'utente può essere esposto al rischio di perdita o furto dei dati. In assenza di uno strumento speciale anti-rootkit, è quasi impossibile rilevarli.

Perché a volte i file contrassegnati come "Firmati da MS" hanno contemporaneamente un "Nome aziendale" differente?

Quando si cerca di identificare la firma digitale di un file eseguibile, ESET SysInspector verifica innanzitutto se nel file è incorporata una firma digitale. Se viene trovata una firma digitale, il file verrà convalidato utilizzando tali informazioni. Se la firma digitale non viene trovata, ESI inizia a ricercare il file CAT corrispondente (Catalogo di protezione - *%systemroot%\system32\catroot*) contenente informazioni sul file eseguibile elaborato. Nel caso in cui dovesse trovare il file CAT appropriato, nel processo di convalida del file eseguibile verrà applicata la firma digitale di tale file CAT.

Per tale motivo, a volte i file contrassegnati come "Firmati da MS" hanno contemporaneamente un "Nome aziendale" differente.

Esempio:

Windows 2000 include l'applicazione HyperTerminal nel percorso *C:\Programmi\Windows NT*. Il file eseguibile dell'applicazione principale non è firmato a livello digitale, ma ESET SysInspector lo contrassegna come file firmato da Microsoft. Ciò dipende da un riferimento in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* che punta a *C:\Programmi\Windows NT\hypertrm.exe* (il principale file eseguibile dell'applicazione HyperTerminal) e *sp4.cat* è firmato a livello digitale da Microsoft.

4.7.8 ESET SysRescue Live

ESET SysRescue Live è un'utilità che consente all'utente di creare un disco di avvio contenente una delle soluzioni ESET Security, tra cui ESET NOD32 Antivirus, ESET Smart Security o alcuni prodotti per server. Il vantaggio principale offerto da ESET SysRescue Live consiste nel fatto che la soluzione ESET Security viene eseguita indipendentemente dal sistema operativo che la ospita ma con un accesso diretto al disco e al file system. Ciò consente di rimuovere infiltrazioni che non sarebbe stato possibile eliminare in una situazione ordinaria, ad esempio, durante l'esecuzione del sistema operativo.

4.7.9 Pianificazione attività

La Pianificazione attività consente di gestire e avviare attività pianificate con configurazioni e proprietà predefinite. La configurazione e le proprietà contengono informazioni quali data e ora, oltre ai profili da utilizzare durante l'esecuzione di un'attività.

È possibile accedere alla Pianificazione attività nella finestra principale del programma di ESET Mail Security facendo clic su **Strumenti** > **Pianificazione attività**. La **Pianificazione attività** contiene un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, ad esempio data, ora e profilo di controllo predefiniti utilizzati.

La Pianificazione attività consente di pianificare le attività seguenti: aggiornamento del database delle firme antivirali, attività di controllo, controllo dei file di avvio del sistema e manutenzione dei rapporti. È possibile aggiungere o eliminare attività direttamente dalla finestra principale Pianificazione attività (fare clic su **Aggiungi attività** o **Elimina**). Fare clic con il pulsante destro del mouse in qualsiasi punto della finestra Pianificazione attività per eseguire le azioni seguenti: visualizzare informazioni dettagliate, eseguire immediatamente l'attività, aggiungere una nuova attività o eliminare un'attività esistente. Utilizzare le caselle di controllo accanto a ciascuna voce per attivare o disattivare le attività.

Per impostazione predefinita, in **Pianificazione attività** vengono visualizzate le attività pianificate seguenti:

- **Manutenzione rapporto**
- **Aggiornamento automatico periodico**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**
- **Controllo automatico file di avvio** (dopo l'accesso utente)
- **Controllo automatico file di avvio** (dopo il completamento dell'aggiornamento del database delle firme antivirali)
- **Primo controllo automatico**

Per modificare la configurazione di un'attività pianificata esistente (predefinita o definita dall'utente), fare clic con il pulsante destro del mouse sull'attività e selezionare **Modifica** oppure selezionare l'attività che si desidera modificare e fare clic su **Modifica**.

Aggiunta di un nuova attività

1. Fare clic su **Aggiungi attività** nella parte inferiore della finestra.

2. Inserire un nome per l'attività.

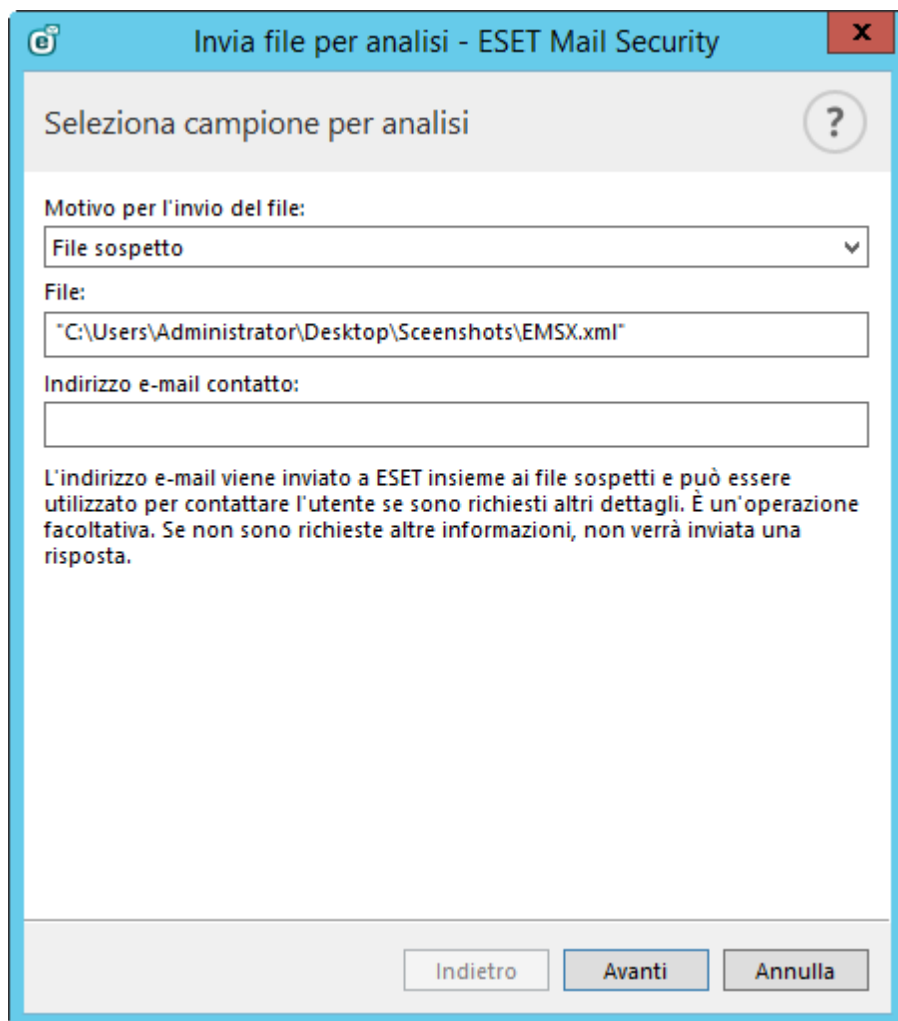
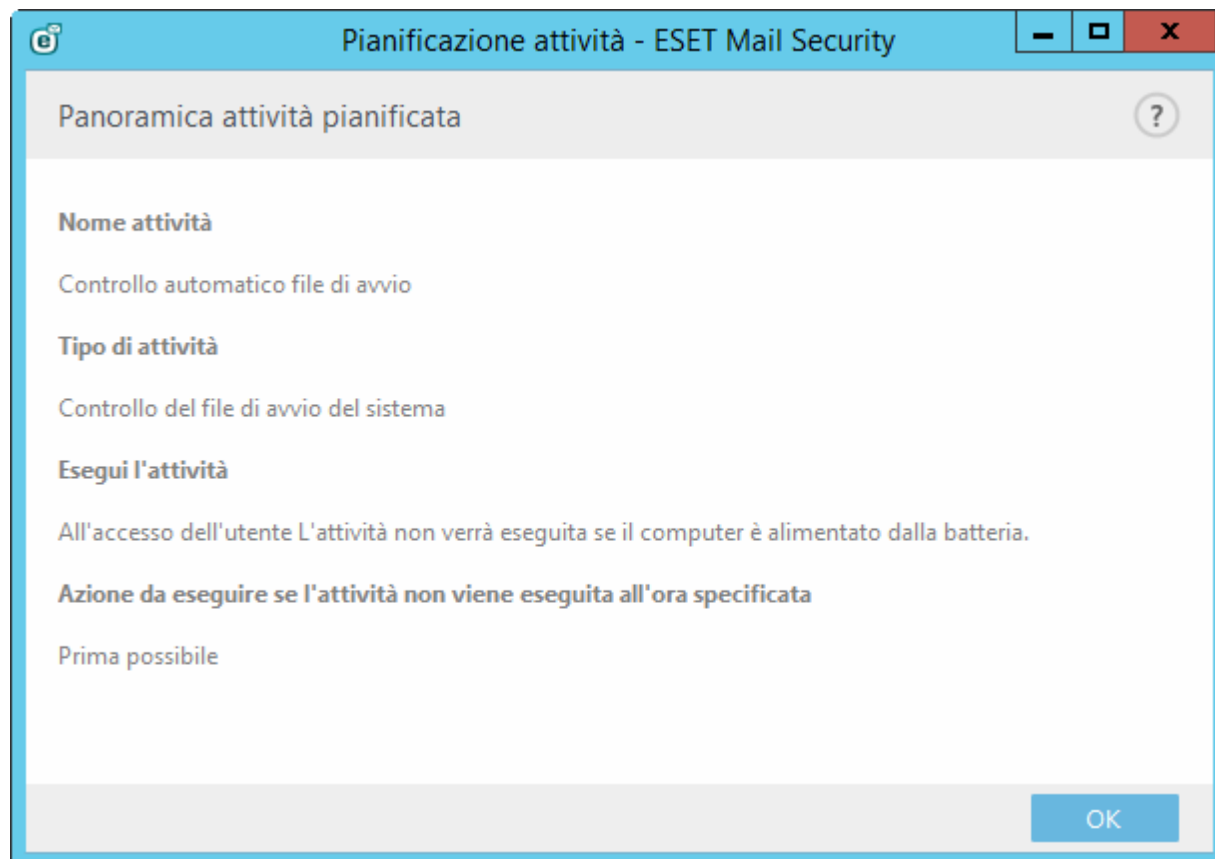
3. Selezionare l'attività desiderata dal menu a discesa:

- **Esegui applicazione esterna**: consente di pianificare l'esecuzione di un'applicazione esterna.
- **Manutenzione rapporto**: file di rapporto contenenti elementi rimasti dai record eliminati. Questa attività ottimizza periodicamente i record nei file di rapporto allo scopo di garantire un funzionamento efficiente.
- **Controllo del file di avvio del sistema**: consente di controllare i file la cui esecuzione è consentita all'avvio del sistema o all'accesso.
- **Crea un controllo computer**: crea uno snapshot ESET SysInspector del computer, raccoglie informazioni dettagliate sui componenti del sistema (ad esempio, driver e applicazioni) e valuta il livello di rischio di ciascun componente.
- **Controllo computer su richiesta**: consente di eseguire un controllo di file e di cartelle sul computer in uso.
- **Primo controllo**: per impostazione predefinita, 20 minuti dopo l'installazione o il riavvio, verrà eseguito un controllo del computer come attività con priorità bassa.
- **Aggiorna**: pianifica un'attività di aggiornamento aggiornando il database delle firme antivirali e i moduli del programma.

4. Fare clic sul pulsante **Attivata** se si desidera attivare l'attività (è possibile eseguire questa operazione in un secondo momento selezionando/deselezionando la casella di controllo nell'elenco di attività pianificate), fare clic su **Avanti** e selezionare una delle opzioni relative alla frequenza di esecuzione:

- **Una volta**: l'attività verrà eseguita alla data e all'ora predefinite.
- **Ripetutamente**: l'attività verrà eseguita in base all'intervallo di tempo specificato.
- **Ogni giorno**: l'attività verrà eseguita ripetutamente ogni giorno all'ora specificata.
- **Ogni settimana**: l'attività verrà eseguita nel giorno e all'ora selezionati.
- **Quando si verifica un evento**: l'attività verrà eseguita quando si verifica un evento specifico.

5. Selezionare **Ignora attività se in esecuzione su un computer alimentato dalla batteria** per ridurre al minimo le risorse di sistema in caso di utilizzo della batteria del computer portatile. L'attività verrà eseguita alla data e all'ora specificate nei campi **Esecuzione attività**. Se l'attività non è stata eseguita all'ora predefinita, è possibile specificare il momento in cui dovrà essere nuovamente eseguita:

- **Al prossimo orario pianificato**
- **Prima possibile**
- **Immediatamente, se l'ora dall'ultima esecuzione supera un valore specificato** (è possibile definire l'intervallo utilizzando la casella di scorrimento **Ora dall'ultima esecuzione**)

Fare clic con il pulsante destro del mouse su un'attività e su **Mostra dettagli attività** dal menu contestuale per visualizzare le informazioni relative all'attività.

4.7.10 Invia campioni per analisi

La finestra di dialogo per l'invio di campioni consente di inviare un file o un sito a ESET ai fini dell'analisi ed è disponibile in **Strumenti** > **Invia campione per l'analisi**. Se è stato trovato un file con un comportamento sospetto nel computer in uso o un sito sospetto su Internet, è possibile inviarlo al laboratorio antivirus ESET per l'analisi. Se il file si rivela essere un'applicazione o un sito Web dannoso, il suo rilevamento verrà aggiunto in un aggiornamento successivo.

In alternativa, è possibile inviare il file tramite e-mail. Per eseguire questa operazione, comprimere i(l) file utilizzando un programma come WinRAR o WinZip, proteggere l'archivio utilizzando la password "infected" e inviarlo a samples@eset.com. Ricordare di inserire una descrizione nel campo dell'oggetto e di fornire il maggior numero di informazioni possibile sul file (ad esempio, l'indirizzo del sito Web dal quale è stato scaricato).

NOTA: prima di inviare un campione a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:

- il file o il sito Web non viene rilevato
- il file o il sito Web viene erroneamente rilevato come minaccia

Non verrà inviata alcuna risposta a meno che non siano richieste ulteriori informazioni ai fini dell'analisi.

Selezionare la descrizione dal menu a discesa **Motivo per l'invio del campione** che si avvicina maggiormente alla propria motivazione:

- **File sospetto**
- **Sito sospetto** (sito Web infettato da un malware)
- **File falso positivo** (file che è stato rilevato come infezione ma che in realtà non è infetto)
- **Sito falso positivo**
- **Altro**

File/sito: percorso del file o del sito Web che si intende inviare.

E-mail contatto: e-mail di contatto che viene inviata a ESET insieme ai file sospetti e può essere utilizzata per contattare l'utente qualora fossero necessarie ulteriori informazioni ai fini dell'analisi. L'immissione dell'indirizzo e-mail di contatto è facoltativa. ESET non invierà alcuna risposta a meno che non siano richieste ulteriori informazioni. Ogni giorno i server ESET ricevono decine di migliaia di file e non è pertanto possibile rispondere a tutti.

4.7.10.1 File sospetto

Segni e sintomi osservati dell'infezione malware: immettere una descrizione del comportamento del file sospetto osservato sul computer.

Origine file (indirizzo URL o fornitore): immettere l'origine e le modalità di ottenimento del file (sorgente).

Note e informazioni aggiuntive: qui è possibile immettere informazioni aggiuntive o una descrizione utile ai fini del processo di identificazione del file sospetto.

i **NOTA:** il primo parametro - **Segni e sintomi osservati dell'infezione malware** - è obbligatorio. Tuttavia, l'invio di informazioni aggiuntive aiuterà i laboratori ESET a potenziare notevolmente le capacità di identificazione dei campioni.

4.7.10.2 Sito sospetto

Selezionare una delle opzioni che seguono dal menu a discesa **Problemi del sito**:

- **Infetto**: sito Web che contiene un virus o un altro malware distribuito con vari metodi.
- **Phishing**: utilizzato solitamente per ottenere l'accesso a dati sensibili, quali numeri di conti bancari, codici PIN e così via. Per ulteriori informazioni su questo tipo di attacco, consultare il glossario.
- **Scam**: sito Web illegale o fraudolento.
- Selezionare **Altro** se le opzioni precedenti non fanno riferimento al sito che si intende inviare.

Note e informazioni aggiuntive: qui è possibile inserire informazioni aggiuntive o una descrizione utile ai fini dell'analisi del sito Web sospetto.

4.7.10.3 File falso positivo

All'utente è richiesto di inviare file rilevati come infezione, ma che in realtà non lo sono, allo scopo di potenziare il motore antivirus e antispyware e garantire la protezione degli altri utenti. I falsi positivi (FP) possono verificarsi quando il criterio di un file corrisponde al criterio contenuto in un database delle firme antivirali.

Nome e versione dell'applicazione: titolo del programma e relativa versione (ad esempio, numero, alias o nome del codice).

Origine file (indirizzo URL o fornitore): specificare un'origine e le modalità di ottenimento del file (sorgente).

Scopo dell'applicazione: descrizione generale dell'applicazione, tipo di applicazione (ad esempio, browser, lettore multimediale e così via) e relative funzionalità.

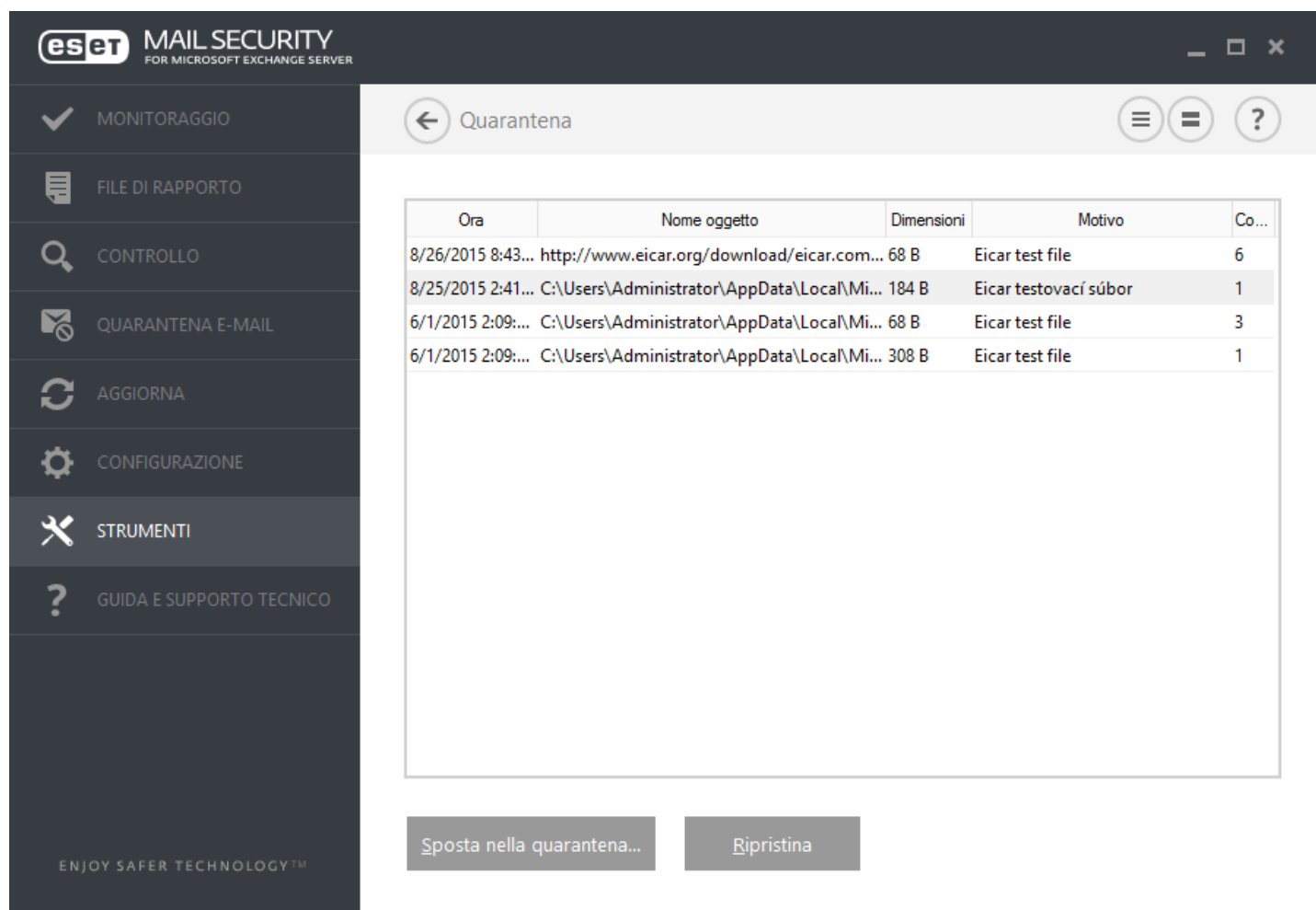
Note e informazioni aggiuntive: qui è possibile inserire informazioni o descrizioni aggiuntive utili ai fini dell'elaborazione del file sospetto.

i **NOTA:** i primi tre parametri sono obbligatori allo scopo di identificare le applicazioni legali e di distinguerle da codice dannoso. L'invio di informazioni aggiuntive aiuterà i laboratori ESET a potenziare notevolmente le capacità di identificazione e di elaborazione dei campioni.

4.7.10.4 Sito falso positivo

Si consiglia di inviare siti rilevati come infezione, scam o phishing ma che in realtà non lo sono. I falsi positivi (FP) possono verificarsi quando il criterio di un file corrisponde al criterio contenuto in un database delle firme antivirali. All'utente è richiesto di segnalare questo sito Web per consentire agli sviluppatori di potenziare il motore antivirus e anti-phishing e per facilitare la protezione degli altri utenti.

Note e informazioni aggiuntive: qui è possibile inserire informazioni o descrizioni aggiuntive utili ai fini dell'elaborazione del file sospetto.

4.7.10.5 Altro

Utilizzare questo modulo se non è possibile classificare il file come **File sospetto** o **Falso positivo**.

Motivo per l'invio del file: immettere una descrizione dettagliata e il motivo dell'invio del file.

4.7.11 Quarantena

La funzione principale della quarantena è archiviare i file infetti in modo sicuro. I file devono essere messi in quarantena se non è possibile pulirli, se non è sicuro o consigliabile eliminarli o, infine, se vengono erroneamente rilevati come minacce da ESET Mail Security.

È possibile mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto ma non viene rilevato dallo scanner antivirus. I file messi in quarantena possono essere inviati al laboratorio antivirus ESET per l'analisi.

I file salvati nella cartella della quarantena possono essere visualizzati in una tabella contenente la data e l'ora della quarantena, il percorso originale del file infetto, la dimensione in byte, il motivo (ad esempio, oggetto aggiunto dall'utente) e il numero di minacce (ad esempio, se si tratta di un archivio contenente più infiltrazioni).

Mettere file in quarantena

ESET Mail Security mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto a disattivare questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti selezionando **Quarantena.** I file della quarantena verranno rimossi dalla loro posizione originale. Per questa operazione è possibile utilizzare anche il menu contestuale: fare clic con il pulsante destro del mouse sulla finestra **Quarantena** e selezionare **Quarantena**.

Ripristino dalla quarantena

È possibile ripristinare nella posizione di origine i file messi in quarantena. Per far ciò, utilizzare la funzione **Ripristina**, disponibile nel menu contestuale, facendo clic con il pulsante destro del mouse sul file desiderato nella finestra Quarantena. Se un file è contrassegnato come applicazione potenzialmente indesiderata, sarà disponibile l'opzione **Ripristina ed escludi dal controllo**. Per ulteriori informazioni su questo tipo di applicazione, consultare la relativa voce del glossario. Il menu contestuale contiene anche l'opzione **Ripristina in...**, che consente di ripristinare i file in una posizione diversa da quella di origine da cui sono stati eliminati.

NOTA: se il programma mette in quarantena per errore un file non dannoso, escludere il file dal controllo dopo averlo ripristinato e inviarlo al Supporto tecnico ESET.

Invio di un file dalla cartella Quarantena

Se un file sospetto che non è stato rilevato dal programma è stato messo in quarantena o se un file è stato segnalato erroneamente come infetto (ad esempio, mediante un'analisi euristica del codice) e quindi messo in quarantena, è necessario inviarlo al laboratorio antivirus ESET. Per inviare un file dalla cartella Quarantena, fare clic con il pulsante destro del mouse su di esso e selezionare **Invia per analisi** dal menu contestuale.

4.8 Guida e supporto tecnico

ESET Mail Security contiene strumenti di risoluzione dei problemi e informazioni di supporto in grado di assistere l'utente nella risoluzione di eventuali problemi che potrebbero insorgere.

Guida

- **Cerca nella Knowledge Base ESET**: la Knowledge Base ESET contiene le risposte alle domande frequenti, nonché le soluzioni consigliate per i vari problemi. Grazie all'aggiornamento periodico effettuato dagli esperti del supporto tecnico di ESET, la Knowledge Base rappresenta lo strumento più potente per risolvere diversi tipi di problemi.
- **Apri Guida**: fare clic su questo collegamento per aprire le pagine della Guida di ESET Mail Security.
- **Trova soluzione rapida**: selezionare questa opzione per trovare le soluzioni ai problemi riscontrati con maggiore frequenza. Si consiglia di leggere questa sezione prima di contattare il Supporto tecnico.

Supporto tecnico

- **Invia richiesta di assistenza**: se non è stata trovata una risposta al problema riscontrato, è anche possibile utilizzare questo modulo disponibile sul sito Web di ESET per contattare rapidamente il Supporto tecnico.

Strumenti di supporto

Enciclopedia delle minacce: contiene un collegamento all'enciclopedia delle minacce ESET, in cui sono presenti informazioni sui pericoli e sui sintomi dei vari tipi di infiltrazioni.

Cronologia database delle firme antivirali: rimanda a ESET Virus Radar, che contiene informazioni sulle versioni del database delle firme antivirali di ESET.

Strumento di pulizia specializzato: questo strumento identifica e rimuove automaticamente le comuni infezioni malware. Per ulteriori informazioni, consultare questo articolo della Knowledge Base ESET.

Informazioni sul prodotto e sulla licenza

- **Informazioni su ESET Mail Security:** consente di visualizzare le informazioni sulla copia di ESET Mail Security.
- Gestisci licenza: selezionare questa opzione per avviare la finestra di attivazione del prodotto. Selezionare uno dei metodi disponibili per attivare ESET Mail Security. Per ulteriori informazioni, consultare Come fare per attivare ESET Mail Security.

4.8.1 Come fare per

In questo capitolo sono illustrate alcune delle domande frequenti e i problemi riscontrati. Fare clic sul titolo dell'argomento per trovare la soluzione al problema:

Come fare per aggiornare ESET Mail Security

Come fare per attivare ESET Mail Security

Come fare per pianificare un'attività di controllo (ogni 24 ore)

Come fare per rimuovere un virus dal server

Come funzionano le esclusioni automatiche

Se il problema non è presente nell'elenco delle pagine della Guida riportate sopra, provare a eseguire una ricerca in base a una parola chiave o frasi che descrivono il problema ed eseguire la ricerca all'interno delle pagine della Guida di ESET Mail Security.

Se non si riesce a trovare la soluzione a un problema o una domanda nelle pagine della Guida, è possibile effettuare una ricerca nella Knowledge Base on-line che viene aggiornata periodicamente.

Se necessario, è possibile contattare direttamente il supporto tecnico online riportando domande o problemi. Il modulo di contatto è disponibile nella scheda Guida e supporto tecnico del programma ESET.

4.8.1.1 Come fare per aggiornare ESET Mail Security

L'aggiornamento di ESET Mail Security può essere eseguito manualmente o automaticamente. Per avviare l'aggiornamento, fare clic su **Aggiorna database delle firme antivirali**, disponibile nella sezione **Aggiorna** del programma.

Le impostazioni predefinite dell'installazione consentono di creare un'attività di aggiornamento automatica che viene eseguita ogni ora. Se occorre modificare l'intervallo, accedere a **Pianificazione attività** (per ulteriori informazioni su Pianificazione attività, fare clic qui).

4.8.1.2 Come fare per attivare ESET Mail Security

Al termine dell'installazione, all'utente verrà richiesto di attivare il prodotto.

Esistono vari metodi per attivare il prodotto. La disponibilità di uno scenario di attivazione specifico nella finestra di attivazione potrebbe variare in base al paese e ai mezzi di distribuzione (CD/DVD, pagina Web ESET, ecc.).

Per attivare la copia di ESET Mail Security direttamente dal programma, fare clic sull'icona della barra delle applicazioni e selezionare **Attiva licenza prodotto** dal menu. È inoltre possibile attivare il prodotto dal menu principale sotto a **Guida e supporto tecnico** > **Attiva Licenza** o **Stato protezione** > **Attiva licenza prodotto**.

Per attivare ESET Mail Security, è inoltre possibile utilizzare uno dei seguenti metodi:

- **Chiave di licenza**: stringa univoca nel formato XXXX-XXXX-XXXX-XXXX-XXXX, utilizzata per l'identificazione del proprietario della licenza e per l'attivazione della stessa.
- Account **Security Admin**: account creato sul portale ESET License Administrator con le credenziali (indirizzo e-mail + password). Questo metodo consente all'utente di gestire licenze multiple da un'unica posizione.
- File della **Licenza off-line**: file generato automaticamente che verrà trasferito al prodotto ESET allo scopo di fornire le informazioni sulla licenza. Il file della licenza off-line viene generato dal portale della licenza e utilizzato in ambienti in cui l'applicazione non può effettuare la connessione all'autorità che ha concesso la

licenza.

Se il computer in uso fa parte di una rete gestita, facendo clic su **Attiva in seguito** con ESET Remote Administrator, l'amministratore eseguirà l'attivazione remota mediante ESET Remote Administrator. È inoltre possibile utilizzare questa opzione qualora si desideri attivare il client in un secondo momento.

Fare clic su **Guida e supporto tecnico** > **Gestisci licenza** nella finestra principale del programma per gestire le informazioni della licenza in qualsiasi momento. Sarà possibile visualizzare l'ID della licenza pubblica per consentire a ESET di identificare il prodotto e ai fini dell'identificazione della licenza. Il nome utente con il quale il computer è registrato nel sistema di gestione delle licenze è archiviato nella sezione **Informazioni su** che comparirà facendo clic con il pulsante destro del mouse sull'icona della barra delle applicazioni .

NOTA: ESET Remote Administrator è in grado di attivare i computer client in modo silenzioso attraverso l'utilizzo delle licenze messe a disposizione dell'amministratore.

4.8.1.3 Come fare per creare una nuova attività in Pianificazione attività

Per creare una nuova attività in **Strumenti** > **Pianificazione attività**, fare clic su **Aggiungi attività** oppure fare clic con il pulsante destro del mouse e selezionare **Aggiungi** dal menu contestuale. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione esterna**: consente di pianificare l'esecuzione di un'applicazione esterna.
- **Manutenzione rapporto**: i file di rapporto contengono anche elementi rimasti dai record eliminati. Questa attività ottimizza periodicamente i record nei file di rapporto allo scopo di garantire un funzionamento efficiente.
- **Controllo del file di avvio del sistema**: consente di controllare i file la cui esecuzione è consentita all'avvio del sistema o all'accesso.
- **Crea uno snapshot dello stato del computer**: crea uno snapshot del computer ESET SysInspector, raccoglie informazioni dettagliate sui componenti del sistema (ad esempio, driver e applicazioni) e valuta il livello di rischio di ciascun componente.
- **Controllo computer su richiesta**: consente di eseguire un controllo di file e di cartelle sul computer in uso.
- **Primo controllo**: per impostazione predefinita, 20 minuti dopo l'installazione o il riavvio, verrà eseguito un Controllo del computer come attività con priorità bassa.
- **Aggiorna**: pianifica un'attività di aggiornamento aggiornando il database delle firme antivirali e i moduli del programma.

Poiché **Aggiorna** rappresenta una delle attività pianificate utilizzata con maggiore frequenza, di seguito verranno illustrate le modalità in cui è possibile aggiungere una nuova attività di aggiornamento:

Dal menu a discesa **Attività pianificata**, selezionare **Aggiorna**. Inserire il nome dell'attività nel campo **Nome attività** e fare clic su **Avanti**. Selezionare la frequenza dell'attività. Sono disponibili le seguenti opzioni: **Una volta**, **Ripetutamente**, **Ogni giorno**, **Ogni settimana** e **Quando si verifica un evento.** Selezionare **Ignora attività se in esecuzione su un computer alimentato dalla batteria** per ridurre al minimo le risorse di sistema in caso di utilizzo della batteria del computer portatile. L'attività verrà eseguita alla data e all'ora specificate nei campi **Esecuzione attività**. È quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le seguenti opzioni:

- **Al prossimo orario pianificato**
- **Prima possibile**
- **Immediatamente, se l'ora dall'ultima esecuzione supera un valore specificato** (è possibile definire l'intervallo utilizzando la casella di scorrimento Ora dall'ultima esecuzione)

Nel passaggio successivo, viene visualizzata una finestra contenente un riepilogo delle informazioni sull'attività pianificata corrente. Fare clic su **Fine** una volta terminate le modifiche.

Verrà visualizzata una finestra di dialogo in cui è possibile scegliere i profili da utilizzare per l'attività pianificata. Qui è possibile impostare il profilo primario e alternativo. Il profilo alternativo viene utilizzato se l'attività non può essere completata mediante l'utilizzo del profilo primario. Confermare facendo clic su **Fine** . A questo punto, la nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

4.8.1.4 Come fare per pianificare un'attività di controllo (ogni 24 ore)

Per programmare un'attività periodica, accedere a **ESET Mail Security** > **Strumenti** > **Pianificazione attività**. Di seguito viene riportata la procedura da seguire per pianificare un'attività che controllerà tutti i dischi locali ogni 24 ore.

Per pianificare un'attività di controllo:

1. Fare clic su **Aggiungi** nella schermata principale di Pianificazione attività.
2. Selezionare **Controllo computer su richiesta** dal menu a discesa.
3. Immettere un nome per l'attività, quindi selezionare **Ripetutamente**.
4. Specificare l'esecuzione dell'attività ogni 24 ore (1440 minuti).
5. Selezionare un'azione da eseguire nel caso in cui, per qualsiasi motivo, non fosse possibile completare l'esecuzione dell'attività.
6. Esaminare il riepilogo dell'attività pianificata e fare clic su **Fine**.
7. Selezionare Unità locali nel menu a discesa **Destinazioni**.
8. Fare clic su **Fine** per confermare l'attività.

4.8.1.5 Come fare per rimuovere un virus dal server

Se il computer mostra sintomi di infezione da malware, ad esempio, appare più lento o si blocca spesso, è consigliabile attenersi alle seguenti istruzioni:

1. Nella finestra principale di ESET Mail Security, fare clic su **Controllo computer**.

2. Fare clic su **Controllo intelligente** per avviare il controllo del sistema.

3. Al termine del controllo, verificare nel registro il numero di file sottoposti a controllo, file infetti e file puliti.

4. Se si desidera controllare solo una parte del disco, scegliere **Controllo personalizzato** e selezionare gli oggetti sui quali eseguire una ricerca di virus.

4.8.2 Invia richiesta di assistenza

Per offrire un servizio di assistenza il più rapido e accurato possibile, ESET richiede informazioni sulla configurazione di ESET Mail Security, informazioni dettagliate sul sistema e i processi in esecuzione (File di rapporto ESET SysInspector) e i dati di registro. ESET utilizzerà questi dati esclusivamente per offrire assistenza tecnica ai propri clienti.

In caso di invio del modulo Web, i dati relativi alla configurazione del sistema verranno inviati a ESET. Selezionare **Invia sempre queste informazioni** se si desidera ricordare questa azione per il processo. Per inviare il modulo senza inviare i dati, fare clic su **Non inviare i dati**: in tal modo, sarà possibile contattare il Supporto tecnico ESET utilizzando il modulo di assistenza on-line.

Questa impostazione può essere configurata anche in **Configurazione avanzata** > **Strumenti** > **Diagnostica** > **Supporto tecnico**.

i **NOTA**: se si è deciso di inviare i dati del sistema, è necessario compilare e inviare il modulo Web. La mancata osservanza di tale istruzione impedirà la creazione della richiesta di assistenza causando la perdita dei dati del sistema.

4.8.3 ESET Specialized Cleaner

ESET Specialized Cleaner è uno strumento di rimozione di infezioni malware comuni, come Conficker, Sirefef o Necurs. Per ulteriori informazioni, consultare questo articolo della Knowledge Base ESET.

4.8.4 Informazioni su ESET Mail Security

In questa finestra vengono fornite informazioni dettagliate sulla versione installata di ESET Mail Security e un elenco dei moduli del programma installati. Nella parte superiore, sono visualizzate le informazioni sul sistema operativo e sulle risorse di sistema.

Per copiare le informazioni sui moduli (**Componenti installati**) negli Appunti, fare clic su **Copia**. Tali informazioni potrebbero essere utili per la risoluzione dei problemi o per contattare il Supporto tecnico.

4.8.5 Attivazione prodotto

Al termine dell'installazione, all'utente verrà richiesto di attivare il prodotto.

Esistono vari metodi per attivare il prodotto. La disponibilità di uno scenario di attivazione specifico nella finestra di attivazione potrebbe variare in base al paese e ai mezzi di distribuzione (CD/DVD, pagina Web ESET, ecc.).

Per attivare la copia di ESET Mail Security direttamente dal programma, fare clic sull'icona della barra delle applicazioni e selezionare **Attiva licenza prodotto** dal menu. È inoltre possibile attivare il prodotto dal menu principale sotto a **Guida e supporto tecnico** > **Attiva Licenza** o **Stato protezione** > **Attiva licenza prodotto**.

Per attivare ESET Mail Security, è inoltre possibile utilizzare uno dei seguenti metodi:

- **Chiave di licenza**: stringa univoca nel formato XXXX-XXXX-XXXX-XXXX-XXXX, utilizzata per l'identificazione del proprietario della licenza e per l'attivazione della stessa.
- Account **Security Admin**: account creato sul portale ESET License Administrator con le credenziali (indirizzo e-mail + password). Questo metodo consente all'utente di gestire licenze multiple da un'unica posizione.
- File della **Licenza off-line**: file generato automaticamente che verrà trasferito al prodotto ESET allo scopo di fornire le informazioni sulla licenza. Il file della licenza off-line viene generato dal portale della licenza e utilizzato in ambienti in cui l'applicazione non può effettuare la connessione all'autorità che ha concesso la licenza.

Se il computer in uso fa parte di una rete gestita, facendo clic su **Attiva in seguito** con ESET Remote Administrator, l'amministratore eseguirà l'attivazione remota mediante ESET Remote Administrator. È inoltre possibile utilizzare questa opzione qualora si desideri attivare il client in un secondo momento.

Fare clic su **Guida e supporto tecnico** > **Gestisci licenza** nella finestra principale del programma per gestire le informazioni della licenza in qualsiasi momento. Sarà possibile visualizzare l'ID della licenza pubblica per consentire a ESET di identificare il prodotto e ai fini dell'identificazione della licenza. Il nome utente con il quale il computer è registrato nel sistema di gestione delle licenze è archiviato nella sezione **Informazioni su** che comparirà facendo clic con il pulsante destro del mouse sull'icona della barra delle applicazioni.

NOTA: ESET Remote Administrator è in grado di attivare i computer client in modo silenzioso attraverso l'utilizzo delle licenze messe a disposizione dell'amministratore.

4.8.5.1 Registrazione

Registrare la licenza completando i campi contenuti nel modulo di registrazione e facendo clic su **Continua**. I campi contrassegnati come obbligatori tra parentesi devono essere necessariamente completati. Queste informazioni verranno utilizzate esclusivamente per motivi legati alla licenza ESET.

4.8.5.2 Attivazione di Security Admin

L'account Security Admin, che viene creato sul portale delle licenze con l'**indirizzo e-mail** e la **password**, è in grado di visualizzare tutte le autorizzazioni delle postazioni. Un account Security Admin consente all'utente di gestire licenze multiple. Se non si possiede un account Security Admin, fare clic su **Crea account** e si verrà reindirizzati alla pagina Web di ESET License Administrator, dove è possibile effettuare la registrazione con le credenziali.

Se si è dimenticata la password, fare clic su **Password dimenticata?** e si verrà reindirizzati al portale ESET Business. Inserire l'indirizzo e-mail e fare clic su **Invia** per confermare. A questo punto, verrà visualizzato un messaggio contenente le istruzioni per la reimpostazione della password.

NOTA: per ulteriori informazioni sull'utilizzo di ESET License Administrator, consultare il manuale dell'utente di ESET License Administrator.

4.8.5.3 Errore di attivazione

L'attivazione di ESET Mail Security non è stata eseguita correttamente. Assicurarsi di aver inserito la **Chiave di licenza** corretta o associato una **Licenza off-line**. Se si è in possesso di una **Licenza off-line** diversa, è necessario inserirla nuovamente. Per verificare la chiave di licenza inserita, fare clic su **ricontrolla la chiave di licenza** o su **acquista una nuova licenza**: in tal modo, si verrà reindirizzati alla pagina Web di ESET dove sarà possibile acquistare una nuova licenza.

4.8.5.4 Licenza

Scegliendo l'opzione di attivazione di Security Admin, all'utente verrà richiesto di selezionare una licenza associata all'account che verrà utilizzato per ESET Mail Security. Fare clic su **Attiva** per continuare.

4.8.5.5 Avanzamento attivazione

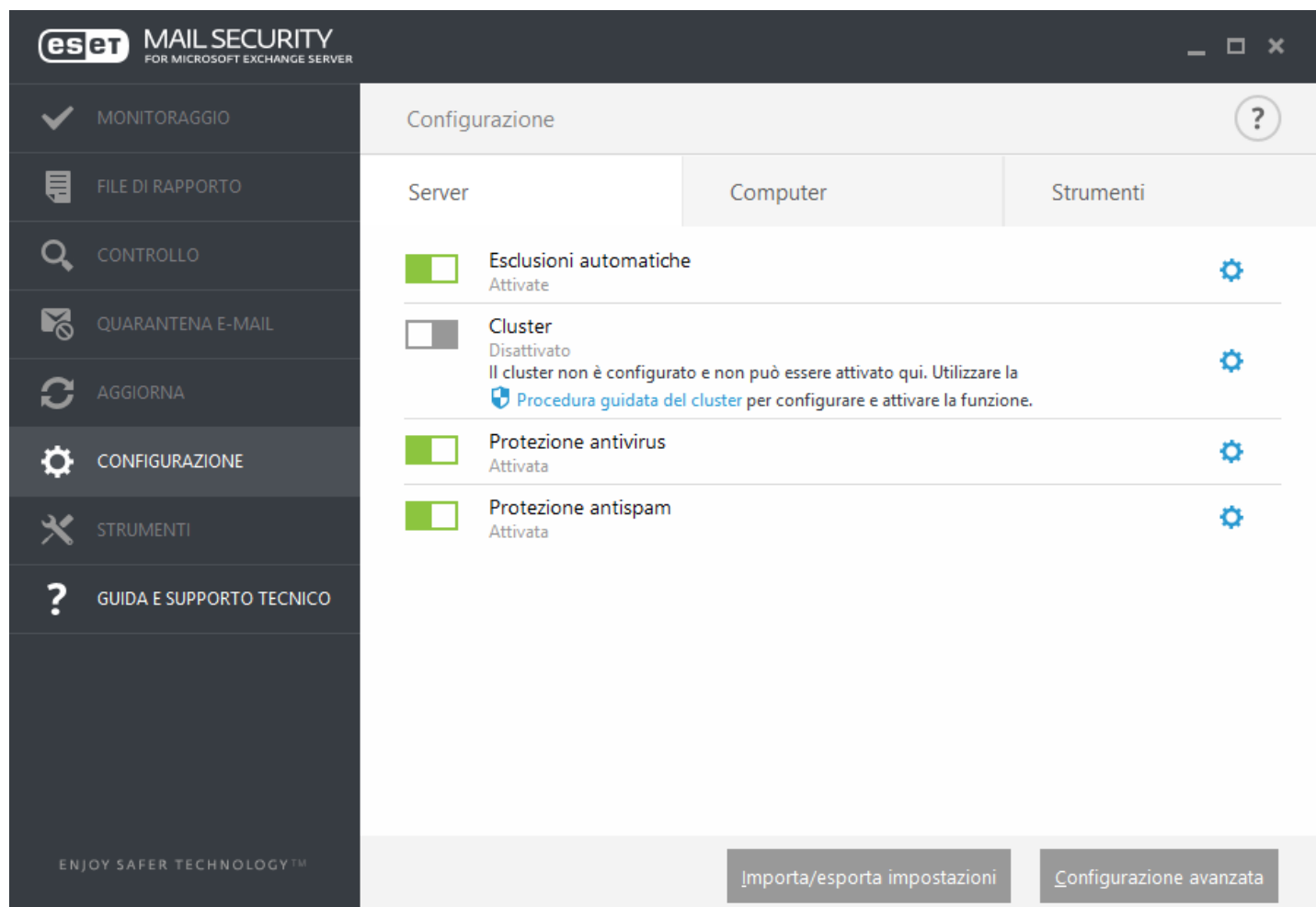
Attivazione di ESET Mail Security in corso, attendere prego. L'operazione potrebbe richiedere qualche minuto.

4.8.5.6 Attivazione avvenuta con successo

L'attivazione è avvenuta correttamente e ESET Mail Security è ora attivo. Da questo punto in poi, ESET Mail Security riceverà aggiornamenti periodici che consentiranno di identificare le ultime minacce e garantire la sicurezza del computer. Fare clic su **Fine** per terminare l'attivazione del prodotto.

5. Utilizzo di ESET Mail Security

Il menu **Configurazione** contiene le sezioni che seguono, che è possibile selezionare mediante le schede:

- Server
- Computer
- Strumenti

Per disattivare temporaneamente i singoli moduli, fare clic sul pulsante verde accanto al modulo desiderato. Tenere presente che in questo modo si potrebbe ridurre il livello di protezione del computer.
Per riattivare la protezione di un componente disattivato, fare clic sul pulsante rosso per far ritornare un componente allo stato attivo.
Per accedere alle impostazioni dettagliate di un particolare componente di sicurezza, fare clic sulla rotella a forma di ingranaggio .

Fare clic su **Configurazione avanzata** o premere **F5** per accedere alle impostazioni e alle opzioni dei componenti aggiuntivi.

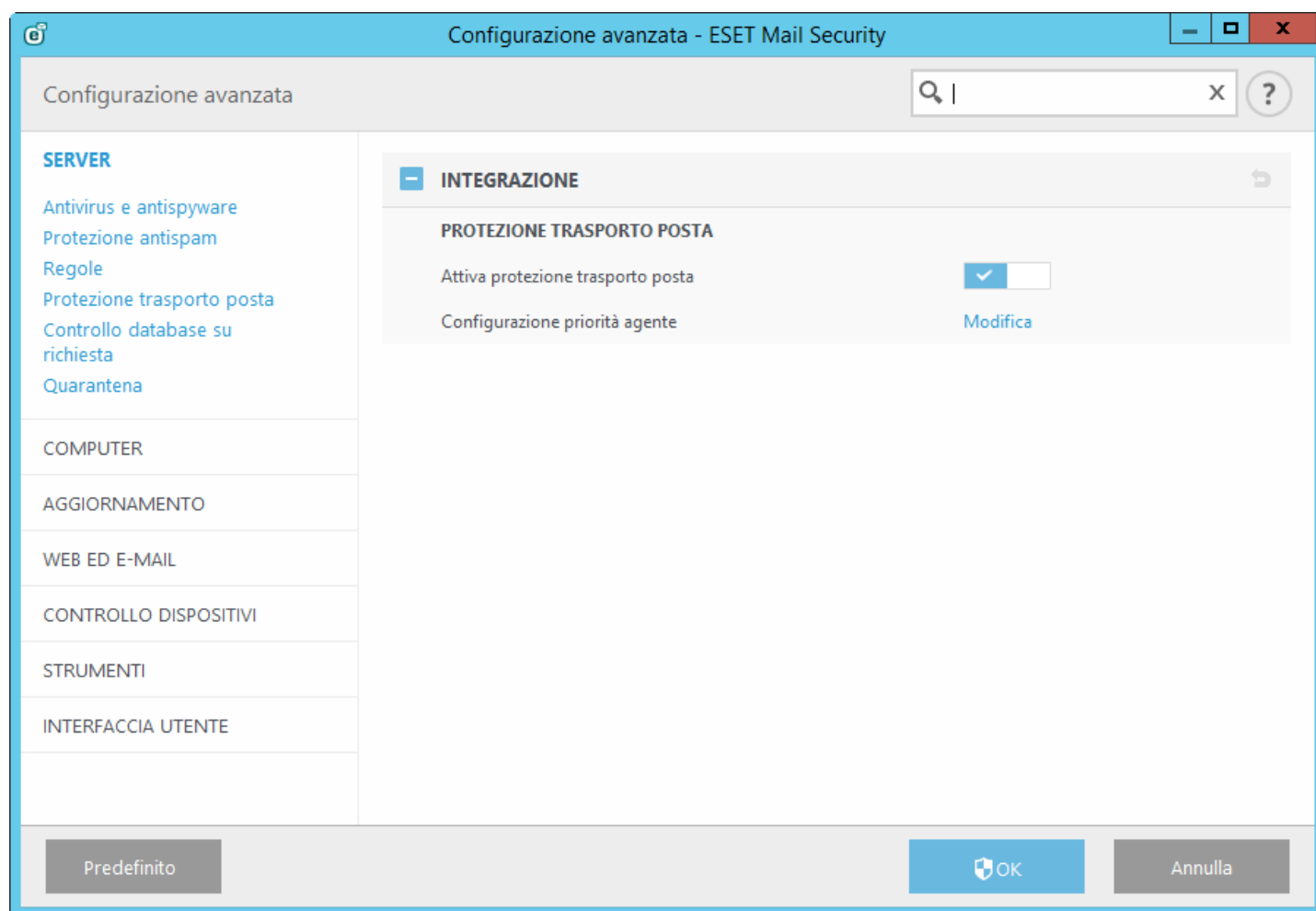
Nella parte inferiore della finestra di configurazione sono disponibili ulteriori opzioni. Utilizzare **Importa/esporta impostazioni** per caricare i parametri di configurazione mediante un file di configurazione *.xml* o per salvare i parametri di configurazione correnti in un file di configurazione. Per ulteriori informazioni, consultare Importa/esporta impostazioni.

5.1 Server

ESET Mail Security offre un importante livello di protezione a Microsoft Exchange Server utilizzando le seguenti funzioni:

- Antivirus e antispyware
- Protezione antispam
- Regole
- Protezione trasporto e-mail (Exchange Server 2007, 2010, 2013)
- Protezione database casella di posta (Exchange Server 2003, 2007, 2010)
- Controllo database su richiesta (Exchange Server 2007, 2010, 2013)
- Quarantena (impostazioni tipi quarantena e-mail)

La sezione Configurazione avanzata consente all'utente di attivare o disattivare l'integrazione della Protezione database casella di posta e della Protezione trasporto e-mail, nonché di modificare la Priorità dell'agente.

NOTA: in caso di esecuzione di Microsoft Exchange Server 2007 o 2010, è possibile scegliere tra la Protezione database casella di posta e il Controllo database su richiesta. Tuttavia, è possibile attivare esclusivamente uno dei due tipi di protezione alla volta. Se si decide di utilizzare il controllo database su richiesta, sarà necessario disattivare l'integrazione della protezione database casella di posta. In caso contrario, il Controllo database su richiesta non sarà disponibile.

5.1.1 Configurazione priorità agente

Nel menu **Configurazione priorità agente** è possibile impostare la priorità in base alla quale gli agenti ESET Mail Security vengono attivati dopo l'avvio di Microsoft Exchange Server. La priorità viene definita da un valore numerico. Minore è il numero, maggiore sarà la priorità. Ciò vale per Microsoft Exchange 2003.

Facendo clic sul pulsante **Modifica** per accedere alla configurazione della priorità dell'agente, è possibile impostare la priorità in base alla quale gli agenti ESET Mail Security vengono attivati dopo l'avvio di Microsoft Exchange Server.

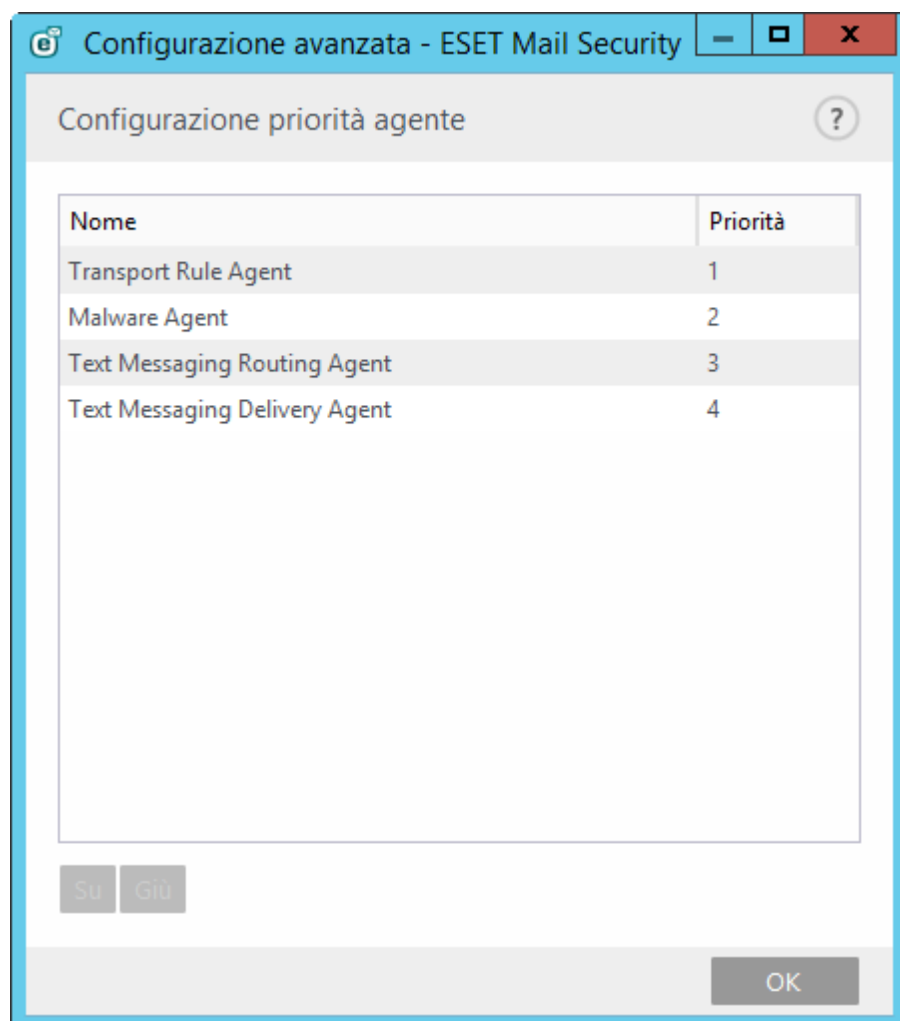
- **Modifica**: definisce manualmente il numero per modificare la priorità dell'agente selezionato.
- **Sposta su**: aumenta la priorità di un agente selezionato spostandolo in alto nell'elenco di agenti.
- **Sposta giù**: diminuisce la priorità di un agente selezionato spostandolo in basso nell'elenco di agenti.

Con Microsoft Exchange Server 2003, è possibile specificare la priorità dell'agente in modo indipendente attraverso l'utilizzo delle schede EOD (fine dei dati) ed RCPT (destinatario).

5.1.1.1 Modifica priorità

In caso di utilizzo di Microsoft Exchange Server 2003, è possibile definire manualmente il numero per la modifica della **Priorità dell'agente di trasporto**. Modificare il numero nel campo testuale o utilizzare le frecce su e giù per modificare la priorità. Minore è il numero, maggiore sarà la priorità.

5.1.2 Configurazione priorità agente

Nel menu **Configurazione priorità agente** è possibile impostare la priorità in base alla quale gli agenti ESET Mail Security vengono attivati dopo l'avvio di Microsoft Exchange Server. Ciò vale per Microsoft Exchange 2007 e versioni successive.

- **Sposta su**: aumenta la priorità di un agente selezionato spostandolo in alto nell'elenco di agenti.

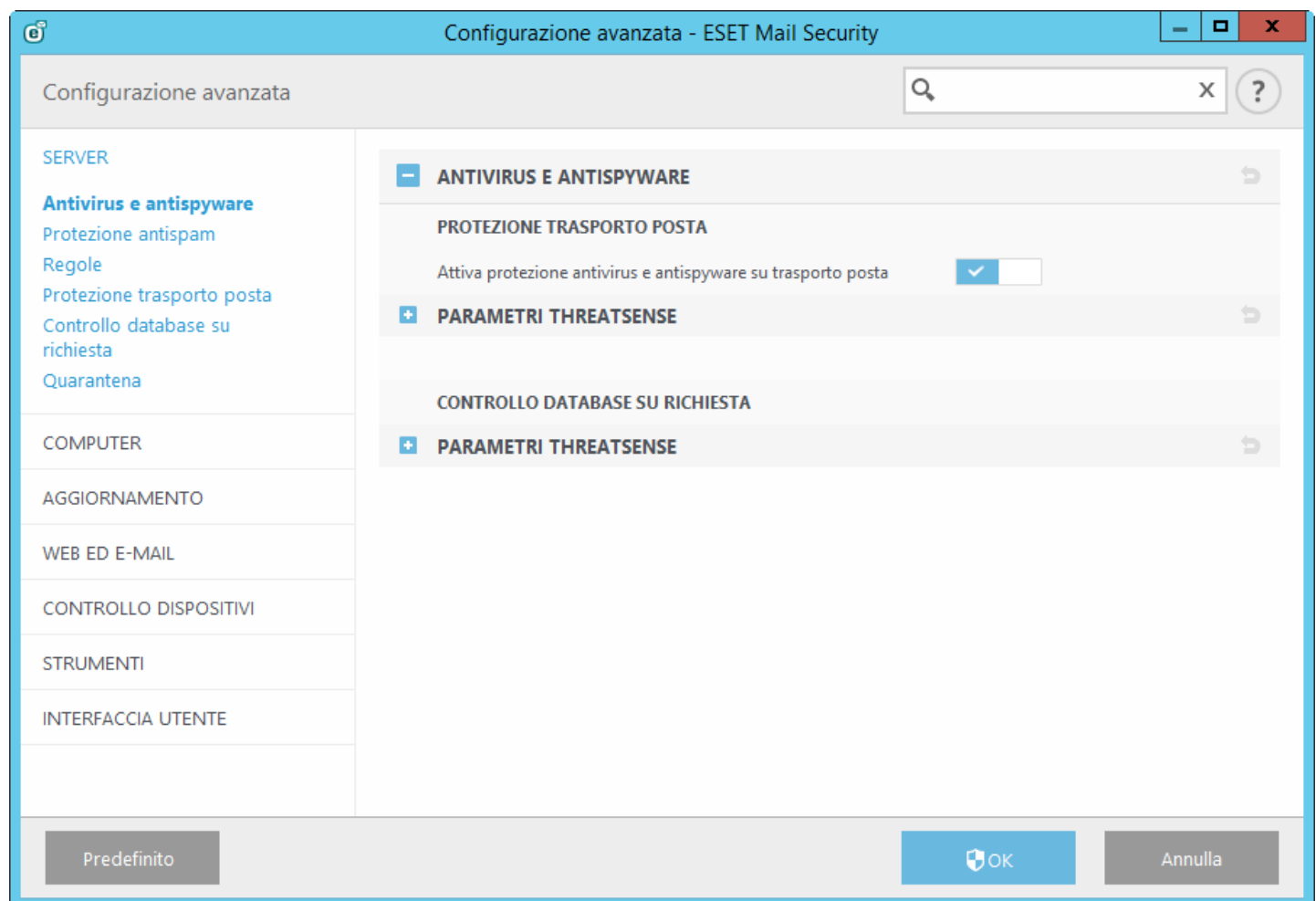
* **Sposta giù**: diminuisce la priorità di un agente selezionato spostandolo in basso nell'elenco di agenti.

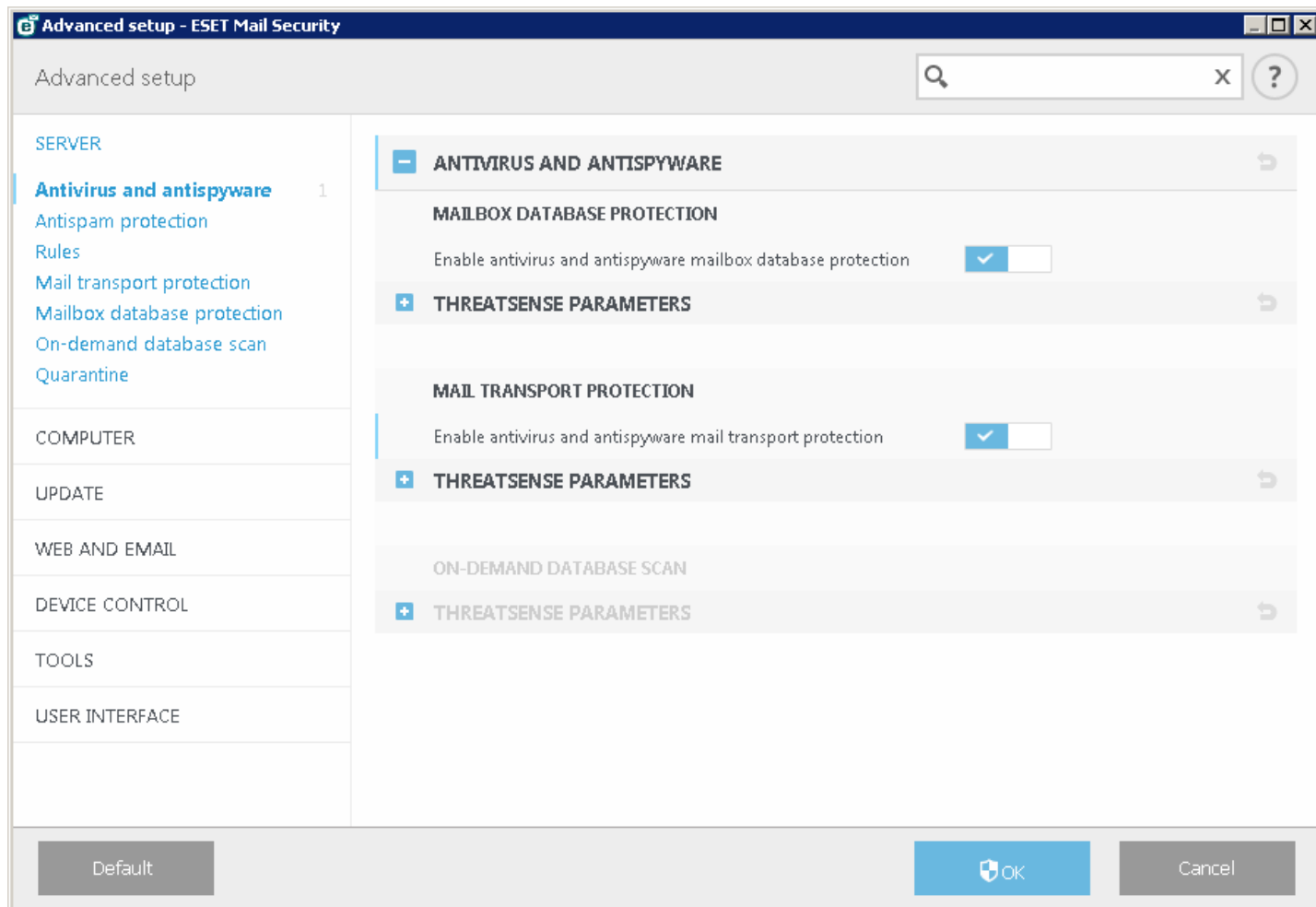
5.1.3 Antivirus e antispyware

In questa sezione è possibile configurare le opzioni **Antivirus e antispyware** per il server di posta in uso.

Importante: la protezione trasporto e-mail è fornita dall'agente di trasporto ed è disponibile esclusivamente per Microsoft Exchange Server 2007 e versioni successive, ma Exchange Server deve possedere il ruolo di Server di trasporto Edge o Server di trasporto Hub. Tale funzione vale anche per l'installazione di un singolo server con ruoli Exchange Server multipli su un computer (a condizione che possieda il ruolo di trasporto Edge o Hub).

Protezione trasporto posta:

disattivando **Attiva protezione antivirus e antispyware su trasporto posta**, il plug-in ESET Mail Security per Exchange Server non verrà scaricato dal processo di Microsoft Exchange Server, ma si limiterà a passare in rassegna i messaggi senza andare alla ricerca di virus a livello di trasporto. Verrà ancora effettuata una ricerca di virus e spam nei messaggi a livello di database e verranno applicate le regole esistenti.

Protezione database casella di posta:

disattivando **Attiva protezione antivirus e antispyware su database casella di posta**, il plug-in ESET Mail Security per Exchange Server non verrà scaricato dal processo di Microsoft Exchange Server, ma si limiterà a passare in rassegna i messaggi senza andare alla ricerca di virus a livello di database. Verrà ancora effettuata una ricerca di virus e spam nei messaggi a livello di database e verranno applicate le regole esistenti.

5.1.4 Protezione antispam

La protezione antispam per il server di posta è attivata per impostazione predefinita. Per disattivarla, fare clic sul pulsante accanto a **Attiva protezione antispam**.

L'attivazione di **Utilizza le whitelist di Exchange Server per disabilitare automaticamente la protezione antispam** consente a ESET Mail Security di utilizzare specifiche "whitelist" di Exchange. Attivando questa opzione, vengono considerati i seguenti elementi:

- L'indirizzo IP del server si trova nell'elenco di IP consentiti di Exchange Server
- Sulla casella di posta del destinatario del messaggio è stato apposto il contrassegno di disabilitazione antispam
- Nell'elenco di mittenti sicuri del destinatario del messaggio è presente l'indirizzo del mittente (assicurarsi di aver configurato la sincronizzazione dell'elenco dei mittenti sicuri nell'ambiente Exchange Server, compresa l'aggregazione dell'elenco di indirizzi attendibili)

Se per un messaggio in entrata vale uno dei casi di cui sopra, il controllo antispam verrà ignorato, non verrà eseguita una valutazione SPAM e il messaggio verrà inviato alla casella di posta del destinatario.

Accetta contrassegno di disabilitazione antispam impostato sulla sessione SMTP è utile in caso di sessioni SMTP autenticate tra i server Exchange con l'impostazione della disabilitazione della protezione antispam. Ad esempio, in presenza di un server Edge e di un server Hub, non è necessario controllare il traffico tra i due server. **Accetta contrassegno di disabilitazione antispam impostato sulla sessione SMTP** è attivato per impostazione predefinita ma si applica solo nel caso in cui il contrassegno di disabilitazione antispam è configurato per la sessione SMTP su Exchange Server. Disattivando **Accetta contrassegno di disabilitazione antispam impostato sulla sessione SMTP**, ESET Mail Security controllerà la presenza di spam nella sessione SMTP indipendentemente dall'impostazione di disabilitazione antispam su Exchange Server.

i **NOTA**: è necessario aggiornare periodicamente il database antispam per consentire al modulo antispam di offrire un livello ottimale di protezione. Per garantire aggiornamenti periodici del database antispam, assicurarsi che ESET Mail Security abbia accesso agli indirizzi IP corretti sulle porte necessarie. Per ulteriori informazioni sugli IP e le

porte da attivare sul firewall di terze parti, consultare questo articolo della Knowledge Base.

5.1.4.1 Filtraggio e verifica

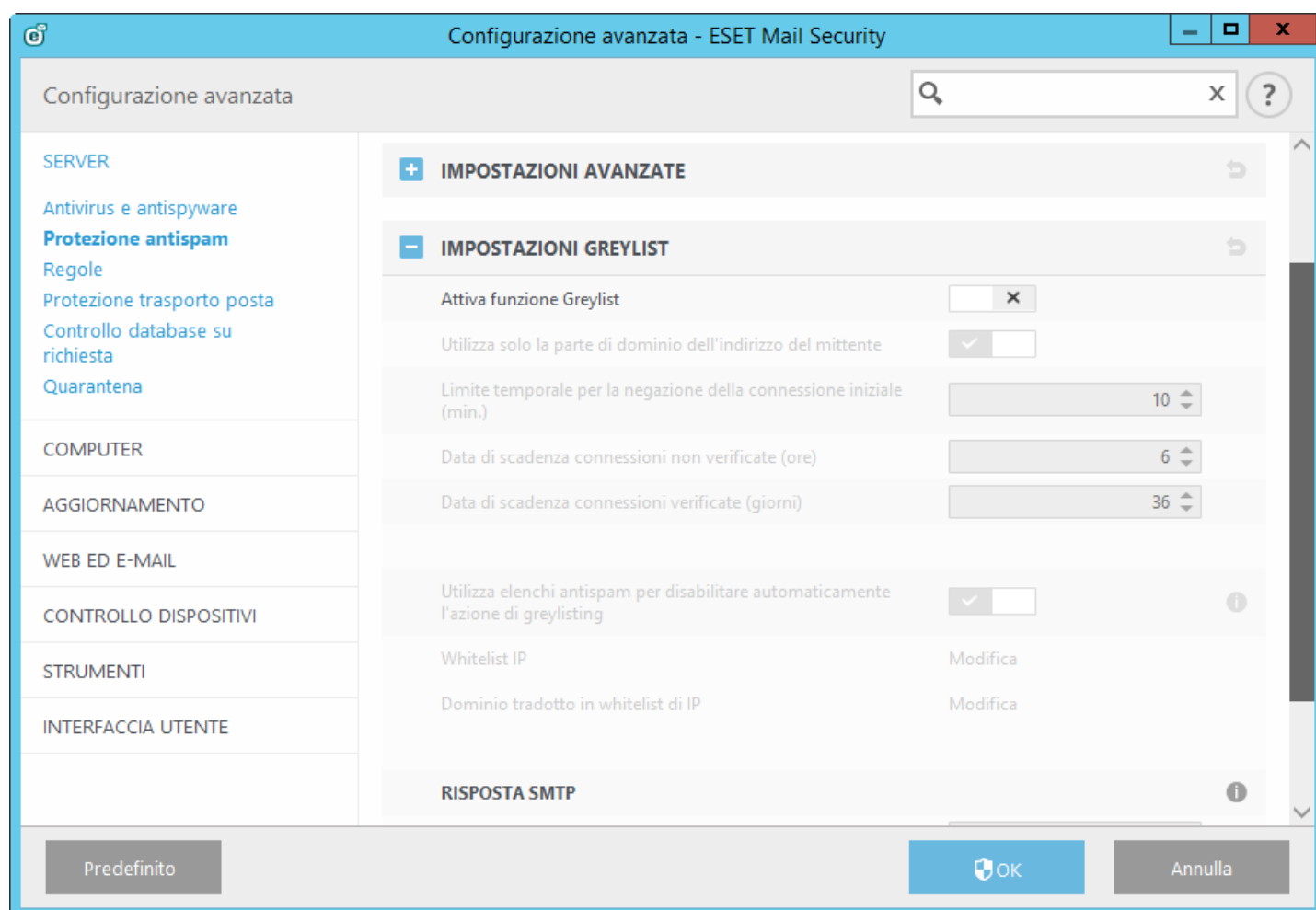
È possibile configurare gli elenchi **Consentiti**, **Bloccati** e **Ignorati** specificando criteri quali l'indirizzo o l'intervallo IP, il nome del dominio, ecc. Per aggiungere, modificare o rimuovere criteri, fare clic su **Modifica** per selezionare l'elenco che si desidera gestire.

- **Elenco di IP approvati**
- **Elenco di IP bloccati**
- **Elenco di IP ignorati**
- **Elenco domini corpo bloccati**
- **Elenco domini corpo ignorati**
- **Elenco IP corpo bloccati**
- **Elenco IP corpo ignorati**
- **Elenco di mittenti approvati**
- **Elenco di mittenti bloccati**
- **Elenco domini su IP approvati**
- **Elenco domini su IP bloccati**
- **Elenco domini su IP ignorati**
- **Elenco set di caratteri bloccati**
- **Elenco Paesi bloccati**

5.1.4.2 Impostazioni avanzate

Queste impostazioni consentono la verifica dei messaggi da parte di server esterni (**RBL** - Realtime Blackhole List, **DNSBL** - DNS Blocklist) in base a criteri definiti.

Limite esecuzione richiesta elenco indirizzi bloccati in tempo reale (RBL) (in secondi): - questa opzione consente all'utente di impostare un tempo massimo per le query RBL. Le risposte RBL vengono utilizzate esclusivamente dai server RBL che rispondono in tempo. Se il valore viene impostato su "0", non viene imposto alcun timeout.

Numero massimo di indirizzi verificati rispetto all'elenco indirizzi bloccati in tempo reale (RBL): - questa opzione consente all'utente di limitare il numero di indirizzi IP per i quali vengono eseguite le query rispetto al server RBL. Si tenga presente che il numero totale di query RBL corrisponderà al numero di indirizzi IP nell'elenco Ricevuti: intestazioni (fino a un massimo di indirizzi IP RBL maxcheck) moltiplicate per il numero di server RBL specificato nell'elenco RBL. Se il valore è impostato su "0", viene controllato un numero illimitato di intestazioni ricevute. Si tenga presente che gli IP presenti nell'elenco di IP ignorati non vengono considerati ai fini del raggiungimento del limite di indirizzi IP RBL.

Limite esecuzione richiesta DNSBL (in secondi): - consente all'utente di impostare un timeout massimo per tutte le query DNSBL da completare.

Numero massimo di indirizzi verificati rispetto al DNSBL: - consente all'utente di limitare il numero di indirizzi IP per i quali vengono eseguite le query rispetto al server DNS Blocklist.

Numero massimo di domini verificati rispetto al DNSBL: - consente all'utente di limitare il numero di domini per i quali vengono eseguite le query rispetto al server DNS Blocklist.

Servizio elenco indirizzi bloccati in tempo reale (RBL): - specifica un elenco di server Realtime Blackhole List (RBL) per i quali eseguire le query durante l'analisi dei messaggi. Per ulteriori informazioni, consultare la sezione RBL di questo documento.

Servizio DNSBL:: specifica un elenco di server DNS Blocklist (DNSBL) per i quali eseguire le query con i domini e gli IP estratti dal corpo del messaggio.

Attiva registrazione diagnostica motore: scrive informazioni dettagliate sul motore antispam nei file di rapporto per scopi diagnostici.

Dimensione massima controllo messaggio (kB): - limita il controllo antispam per i messaggi più grandi rispetto al valore specificato. Questi messaggi non verranno controllati dal motore antispam.

5.1.4.3 Impostazioni greylist

Il comando **Attiva funzione greylist** attiva una funzione che protegge gli utenti dai messaggi spam utilizzando la tecnica seguente: L'agente di trasporto invierà un valore di ritorno SMTP "rifiuta temporaneamente" (valore predefinito: 451/4.7.1) per ogni e-mail ricevuta non proveniente da un mittente riconosciuto. Un server legittimo tenterà di inviare nuovamente il messaggio dopo un certo ritardo. Tipicamente, i server di spam non tenteranno di inviare nuovamente il messaggio, ma passeranno in rassegna migliaia di indirizzi e-mail senza perdere tempo per il rinvio. La funzione greylist rappresenta un livello aggiuntivo di protezione antispam, che non incide sulle capacità di valutazione dei messaggi spam del modulo antispam.

Durante la valutazione dell'origine del messaggio, il metodo greylist tiene conto dell'**Elenco di IP approvati**, dell'**Elenco di IP ignorati**, dei **Mittenti sicuri** e degli **Elenchi di IP consentiti** sul server Exchange, nonché delle impostazioni AntispamBypass per la casella di posta del destinatario. Le e-mail provenienti da questi elenchi di indirizzi IP/mittenti o di e-mail inviati a una casella di posta sulla quale è attivata l'opzione AntispamBypass verranno ignorate dal metodo di rilevamento greylist.

Utilizza solo la parte di dominio dell'indirizzo del mittente: ignora il nome del destinatario nell'indirizzo e-mail e considera solo il dominio.

Limite temporale per la negazione della connessione iniziale (min.): nel momento in cui un messaggio viene inviato per la prima volta e rifiutato temporaneamente, questo parametro definisce il periodo di tempo durante il quale il messaggio sarà sempre rifiutato (misurato a partire dal primo rifiuto). Al termine del periodo di tempo definito, il messaggio verrà ricevuto correttamente. Il valore minimo che è possibile indicare è 1 minuto.

Data di scadenza connessioni non verificate (ore): questo parametro definisce l'intervallo temporale minimo durante il quale verranno archiviati i dati della tripletta. Prima del termine di questo periodo di tempo, è necessario che un server valido invii nuovamente un messaggio desiderato. Questo valore deve essere superiore al valore relativo al **Limite temporale per la negazione della connessione iniziale**.

Data di scadenza connessioni verificate (giorni):: numero di giorni minimo durante il quale vengono archiviate le informazioni della tripletta e le e-mail provenienti da uno specifico mittente verranno ricevute senza ritardi. Questo valore deve essere superiore al valore relativo alla **Data di scadenza connessioni non verificate**.

Risposta SMTP (per le connessioni temporaneamente negate): è possibile specificare un **Codice risposta**, un **Codice stato** e un **Messaggio risposta**, che definiscono la risposta di rifiuto temporanea SMTP inviata al server SMTP in caso di rifiuto di un messaggio.

Esempio di messaggio di risposta di rifiuto SMTP:

Codice risposta	Codice stato	Messaggio risposta
451	4.7.1	Azione richiesta ignorata: errore locale durante l'elaborazione

AVVISO: una sintassi non corretta nei codici di risposta SMTP potrebbe causare malfunzionamenti della protezione greylist. Di conseguenza, i messaggi di spam potrebbero essere inviati ai client o non essere affatto inviati.

NOTA: durante la definizione della risposta di rifiuto SMTP è anche possibile utilizzare le variabili di sistema.

5.1.5 Regole

Le **Regole** consentono agli amministratori di definire manualmente le condizioni di filtraggio delle e-mail e le azioni da intraprendere con le e-mail filtrate.

Sono disponibili tre set separati di regole. Le regole disponibili nel sistema in uso dipendono dalla versione di Microsoft Exchange Server installata sul server con ESET Mail Security:

- Protezione database casella di posta: questo tipo di protezione è disponibile esclusivamente per Microsoft Exchange Server 2010, 2007 e 2003 che operano nel ruolo di Server della casella di posta (Microsoft Exchange 2010 e 2007) o di Server back-end (Microsoft Exchange 2003). Questo tipo di controllo viene eseguito sull'installazione di un singolo server con ruoli Exchange Server multipli su un computer (a condizione che sia presente il ruolo casella di posta o back-end).
- Protezione trasporto posta: questa protezione viene offerta dall'agente di trasporto ed è disponibile esclusivamente per Microsoft Exchange Server 2007 o versioni successive che operano nel ruolo di Server di trasporto Edge o di Server di trasporto Hub. Questo tipo di controllo viene eseguito sull'installazione di un singolo server con ruoli Exchange Server multipli su un computer (a condizione che sia presente uno dei ruoli del server indicati in precedenza).
- Controllo database su richiesta: consente all'utente di eseguire o pianificare un controllo del database delle caselle di posta di Exchange. Questa funzione è disponibile esclusivamente per Microsoft Exchange Server 2007 o versioni successive che operano nel ruolo di Server della casella di posta o di Trasporto Hub. Tale funzione si applica anche all'installazione di un singolo server con ruoli Exchange Server multipli su un computer (a condizione che sia presente uno dei ruoli del server indicati in precedenza). Consultare Ruoli di Exchange Server 2013 per maggiori informazioni sui ruoli in Exchange 2013.

5.1.5.1 Elenco regole

Una regola si basa su **condizioni** e **azioni**. Nel momento in cui vengono soddisfatte tutte le condizioni di un messaggio e-mail, verranno intraprese alcune azioni. In altre parole, le regole vengono applicate in base a un set di condizioni combinate. Se, per una regola, esistono condizioni multiple, queste verranno combinate mediante l'utilizzo dell'operatore logico E e la regola verrà applicata esclusivamente se le condizioni vengono soddisfatte.

La finestra dell'elenco **Regole** consente di visualizzare le regole esistenti. Le regole vengono classificate in base a tre livelli e valutate nel seguente ordine:

- **Regole di filtraggio (1)**
- **Regole elaborazione allegati (2)**
- **Regole elaborazione risultati (3)**

Le regole caratterizzate da uno stesso livello vengono valutate nell'ordine in cui sono visualizzate nella finestra Regole. È possibile modificare esclusivamente l'ordine delle regole dello stesso livello. Ad esempio, in presenza di regole di Filtraggio multiple, è possibile modificare l'ordine di applicazione. Non è invece possibile modificare l'ordine posizionando le regole di Elaborazione allegati prima delle regole di Filtraggio e i pulsanti Su/Giù non saranno disponibili. In altre parole, non è possibile mescolare regole di livelli diversi.

La colonna Risultati consente di visualizzare il numero di volte in cui la regola è stata applicata correttamente. Deselezionando una casella di controllo (sulla sinistra del nome di ciascuna regola), verrà disattivata la regola corrispondente finché la casella di controllo non verrà nuovamente selezionata.

- **Aggiungi...** : aggiunge una nuova regola
- **Modifica...** - modifica una regola esistente
- **Rimuovi**: rimuove la regola selezionata
- **Sposta su**: sposta la regola selezionata in alto nell'elenco
- **Sposta giù**: sposta la regola selezionata in basso nell'elenco
- **Azzera**: azzera il contatore della regola selezionata (la colonna Risultati)

NOTA: in caso di aggiunta di una nuova regola o di modifica di una regola esistente, verrà riavviato automaticamente un controllo del messaggio mediante l'utilizzo delle regole nuove/modificate.

Le regole vengono controllate in base a un messaggio elaborato dall'agente di trasporto (TA) o VSAPI. Se TA e VSAPI sono entrambi attivati e il messaggio corrisponde alle condizioni della regola, il contatore delle regole potrebbe aumentare di 2 o più valori. Ciò dipende dal fatto che VSAPI accede separatamente al corpo e all'allegato di un messaggio e, di conseguenza, le regole vengono applicate a ciascuna parte in modo indipendente. Le regole vengono anche applicate durante il controllo in background (ad esempio, se ESET Mail Security esegue un controllo della casella di posta in seguito al download di un nuovo database delle firme antivirali), che determina un aumento del conteggio delle regole.

5.1.5.1.1 Procedura guidata regole

È possibile definire le **Condizioni** e le **Azioni** utilizzando la procedura guidata **Regole**. Definire prima le condizioni e poi le azioni. Facendo clic su **Aggiungi** comparirà la finestra Condizioni regole, dove è possibile selezionare il tipo di condizione, l'operazione e il valore. Da qui è possibile aggiungere un'Azione della regola. Dopo aver definito azioni e condizioni, digitare un **Nome** per la regola (tramite il quale sarà possibile riconoscere la regola) che verrà visualizzato nell'Elenco di regole. Se si desidera preparare le regole ma si prevede di utilizzarle in un secondo momento, fare clic sul pulsante accanto a **Attiva** per disattivare la regola. Per attivare la regola, selezionare la casella di controllo posizionata accanto nell'Elenco di regole.

Alcune **Condizioni** e **Azioni** differiscono per le regole relative alla **Protezione trasporto e-mail**, alla **Protezione database casella di posta** e al **Controllo database su richiesta**. Ciò dipende dal fatto che ciascun tipo di protezione utilizza un approccio leggermente diverso durante l'elaborazione dei messaggi, specialmente nel caso della **Protezione trasporto e-mail**.

5.1.5.1.1.1 Condizione regola

La procedura guidata consente all'utente di aggiungere le condizioni di una regola. Selezionare **Tipo** > **Operazione** dall'elenco a discesa (l'elenco di operazioni cambia in base al tipo di regola scelto) e **Parametro**. **I campi dei** Parametri cambieranno in base al tipo di regola e all'operazione.

Ad esempio, scegliere **Dimensione allegato** > **è maggiore di** e specificare 10 MB in **Parametro**. Utilizzando queste impostazioni, i messaggi contenenti un allegato maggiore di 10 MB verranno elaborati mediante l'utilizzo dell'azione della regola specificata. Per questo motivo, è necessario specificare l'azione intrapresa in caso di attivazione di una data regola qualora tale operazione non sia stata eseguita durante l'impostazione dei parametri per quella specifica regola.

NOTA: è possibile aggiungere più di una condizione per ciascuna regola. In caso di aggiunta di più di una condizione, non verranno visualizzate le condizioni che si annullano a vicenda.

Le seguenti **Condizioni** sono disponibili per la **Protezione trasporto e-mail** (alcune opzioni potrebbero non essere visualizzate in base alle condizioni selezionate in precedenza):

- **Oggetto**: si applica ai messaggi che contengono o non contengono una specifica stringa (o espressione regolare) nell'oggetto.
- **Mittente**: si applica ai messaggi inviati da un mittente specifico
- **Destinatario**: si applica ai messaggi inviati a un destinatario specifico
- **Nome allegato**: si applica ai messaggi contenenti allegati con un nome specifico
- **Dimensione allegato**: si applica ai messaggi con un allegato che non presenta una specifica dimensione, rientra in un intervallo di dimensioni specifico o supera una dimensione specifica
- **Tipo di allegato**: si applica ai messaggi con uno specifico tipo di file allegato. I tipi di file sono categorizzati in gruppi per una più agevole selezione. È possibile selezionare tipi di file multipli o intere categorie
- **Dimensione messaggio**: si applica ai messaggi con allegati che non presentano una specifica dimensione, rientrano in un intervallo di dimensioni specifico o superano una dimensione specifica
- **Risultato controllo antispam**: si applica ai messaggi contrassegnati o non contrassegnati come Ham o Spam
- **Risultato controllo antivirus**: si applica ai messaggi contrassegnati come dannosi o non dannosi
- **Messaggio interno**: si applica in base al fatto che un messaggio sia o meno interno
- **Data di ricezione**: si applica ai messaggi ricevuti prima o dopo una specifica data o durante un intervallo di date specifico
- **Intestazioni messaggio**: si applica ai messaggi la cui intestazione contiene dati specifici
- **Contiene archivio protetto con password**: si applica ai messaggi a cui sono allegati archivi protetti con password
- **Contiene archivio danneggiato**: si applica ai messaggi a cui sono allegati archivi danneggiati (con molta probabilità impossibili da aprire)
- **Indirizzo IP mittente**: si applica ai messaggi inviati da un indirizzo IP specifico
- **Dominio mittente**: si applica ai messaggi inviati da un mittente con un dominio specifico negli indirizzi di posta
- **Unità aziendali destinatario**: si applica ai messaggi inviati a un destinatario di una specifica unità aziendale

Elenco di Condizioni disponibili per la Protezione database casella di posta e il Controllo database su richiesta (alcune delle opzioni potrebbero non essere visualizzate in base alle condizioni selezionate in precedenza):

- **Oggetto**: si applica ai messaggi che contengono o non contengono una specifica stringa (o espressione regolare) nell'oggetto.

- **Mittente**: si applica ai messaggi inviati da un mittente specifico
- **Destinatario**: si applica ai messaggi inviati a un destinatario specifico
- **Casella di posta**: si applica ai messaggi posizionati in una casella di posta specifica
- **Nome allegato**: si applica ai messaggi contenenti allegati con un nome specifico
- **Dimensione allegato**: si applica ai messaggi con un allegato che non presenta una specifica dimensione, rientra in un intervallo di dimensioni specifico o supera una dimensione specifica
- **Tipo di allegato**: si applica ai messaggi con uno specifico tipo di file allegato. I tipi di file sono categorizzati in gruppi per una più agevole selezione. È possibile selezionare tipi di file multipli o intere categorie
- **Risultato controllo antivirus** - **Risultato controllo antivirus**: si applica ai messaggi contrassegnati come dannosi o non dannosi
- **Data di ricezione**: si applica ai messaggi ricevuti prima o dopo una specifica data o durante un intervallo di date specifico
- **Intestazioni messaggio**: si applica ai messaggi la cui intestazione contiene dati specifici
- **Contiene archivio protetto con password**: si applica ai messaggi a cui sono allegati archivi protetti con password
- **Contiene archivio danneggiato**: si applica ai messaggi a cui sono allegati archivi danneggiati (con molta probabilità impossibili da aprire)
- **Indirizzo IP mittente**: si applica ai messaggi inviati da un indirizzo IP specifico
- **Dominio mittente**: si applica ai messaggi inviati da un mittente con un dominio specifico negli indirizzi di posta

5.1.5.1.1.2 Azione regola

È possibile aggiungere azioni che verranno eseguite con i messaggi e/o gli allegati che corrispondono alle condizioni delle regole.

NOTA: è possibile aggiungere più di una condizione per ciascuna regola. In caso di aggiunta di più di una condizione, non verranno visualizzate le condizioni che si annullano a vicenda.

L'elenco di **Azioni** disponibili per la **Protezione trasporto e-mail** (alcune opzioni potrebbero non essere visualizzate in base alle condizioni selezionate):

- **Messaggio quarantena**: il messaggio non verrà consegnato al destinatario e verrà spostato nella quarantena e-mail
- **Elimina allegato:** elimina l'allegato di un messaggio che verrà pertanto inviato al destinatario senza allegato
- **Rifiuta messaggio**: il messaggio non verrà consegnato e al destinatario verrà inviato un NDR (rapporto di mancato recapito)
- **Elimina automaticamente messaggio**: elimina un messaggio senza inviare un NDR
- **Imposta valore SCL**: modifica o imposta uno specifico valore SCL
- **Invia report**: invia un report
- **Salta controllo antispam**: il messaggio verrà controllato dal motore antispam
- **Salta controllo antivirus**: il messaggio verrà controllato dal motore antivirus
- **Valuta altre regole**: valuta altre regole, consentendo all'utente di definire set multipli di condizioni e azioni multiple da intraprendere in base alle condizioni
- **Rapporto:** scrive informazioni sulla regola applicata al rapporto del programma

- **Aggiungi intestazione archiviata**: aggiunge una stringa personalizzata nell'intestazione di un messaggio

Elenco di **Azioni** disponibili per la **Protezione database casella di posta** e il **Controllo database su richiesta** (alcune opzioni potrebbero non essere visualizzate in base alle condizioni selezionate):

- **Elimina allegato:** elimina l'allegato di un messaggio che verrà pertanto inviato al destinatario senza allegato
- **Metti allegato in quarantena**: mette l'allegato dell'e-mail nella quarantena e-mail; l'e-mail verrà pertanto consegnata al destinatario senza allegato
- **Sostituisci allegato con informazioni sull'azione**: rimuove un allegato e aggiunge informazioni sull'azione intrapresa con l'allegato al corpo dell'e-mail
- **Elimina messaggio**: elimina il messaggio
- **Invia report**: invia un report
- **Salta controllo antivirus**: il messaggio verrà controllato dal motore antivirus
- **Valuta altre regole**: valuta altre regole, consentendo all'utente di definire set multipli di condizioni e azioni multiple da intraprendere in base alle condizioni
- **Rapporto:** scrive informazioni sulla regola applicata al rapporto del programma
- **Sposta messaggio nel cestino** (disponibile solo per il **Controllo database su richiesta**): mette un messaggio e-mail nella cartella del cestino lato client di posta

5.1.6 Protezione database cassetta postale

Nei seguenti sistemi la **Protezione database casella postale** è disponibile in **Impostazioni avanzate** > **Server**:

- Microsoft Exchange Server 2003 (ruolo di server back-end)
- Microsoft Exchange Server 2003 (installazione di server singolo con ruoli multipli)
- Microsoft Exchange Server 2007 (ruolo di server casella di posta)
- Microsoft Exchange Server 2007 (installazione di server singolo con ruoli multipli)
- Microsoft Exchange Server 2010 (ruolo di server casella di posta)
- Microsoft Exchange Server 2010 (installazione di server singolo con ruoli multipli)
- Windows Small Business Server 2003
- Windows Small Business Server 2008
- Windows Small Business Server 2011

NOTA: la Protezione database casella di posta non è disponibile per Microsoft Exchange Server 2013.

Deselezionando **Attiva protezione antivirus e antispyware VSAPI 2.6**, il plug-in ESET Mail Security per il server Exchange non verrà scaricato dal processo del server Microsoft Exchange, ma si limiterà a passare in rassegna i messaggi senza ricercare virus. Tuttavia, verranno ancora ricercati messaggi di spam e verranno applicate le regole.

Attivando il **Controllo proattivo**, i nuovi messaggi in entrata verranno controllati in base all'ordine di ricezione. Se questa opzione viene attivata e un utente apre un messaggio che non è stato ancora controllato, su questo messaggio verrà avviato un controllo prima degli altri messaggi presenti nella coda.

Il **Controllo in background** consente di controllare tutti i messaggi da eseguire in background (il controllo viene eseguito sulla casella di posta e nell'archivio delle cartelle pubbliche, ad esempio sul database Exchange). Microsoft Exchange Server decide se verrà o meno eseguito un controllo in background sulla base di vari fattori quali il carico di sistema corrente, il numero di utenti attivi, ecc. Microsoft Exchange Server mantiene un record di messaggi controllati e della versione del database delle firme antivirali utilizzata. In caso di apertura di un messaggio che non è stato controllato dal database di firme antivirali più recente, Microsoft Exchange Server invierà il messaggio a ESET Mail Security, che lo controllerà prima dell'apertura nel client di posta. È possibile scegliere di **Controllare solo messaggi con allegato** e di applicare il filtro in base al tempo di ricezione mediante l'utilizzo delle seguenti opzioni relative al **Livello di controllo**:

- **Tutti i messaggi**
- **Messaggi ricevuti entro lo scorso anno**
- **Messaggi ricevuti entro gli ultimi 6 mesi**
- **Messaggi ricevuti entro gli ultimi 3 mesi**
- **Messaggi ricevuti entro gli ultimi mesi**
- **Messaggi ricevuti entro l'ultima settimana**

Dal momento che il controllo in background incide sul carico di sistema (il controllo viene eseguito in seguito a ciascun aggiornamento del database delle firme antivirali), si consiglia di pianificare l'esecuzione dei controlli al di fuori degli orari di lavoro. Il controllo in background pianificato può essere configurato mediante una speciale attività nella Pianificazione attività/Utilità di pianificazione. Durante la pianificazione di un'attività di controllo in background, è possibile impostare l'ora di avvio, il numero di ripetizioni e altri parametri disponibili nella Pianificazione attività/Utilità di pianificazione. Dopo averla pianificata, l'attività comparirà nell'elenco di attività pianificate e sarà possibile modificarne i parametri, eliminarla o disattivarla temporaneamente.

L'attivazione dell'opzione **Controlla corpi messaggi RTF** determina l'attivazione del controllo dei corpi dei messaggi RTF. I corpi dei messaggi RTF possono contenere virus delle macro.

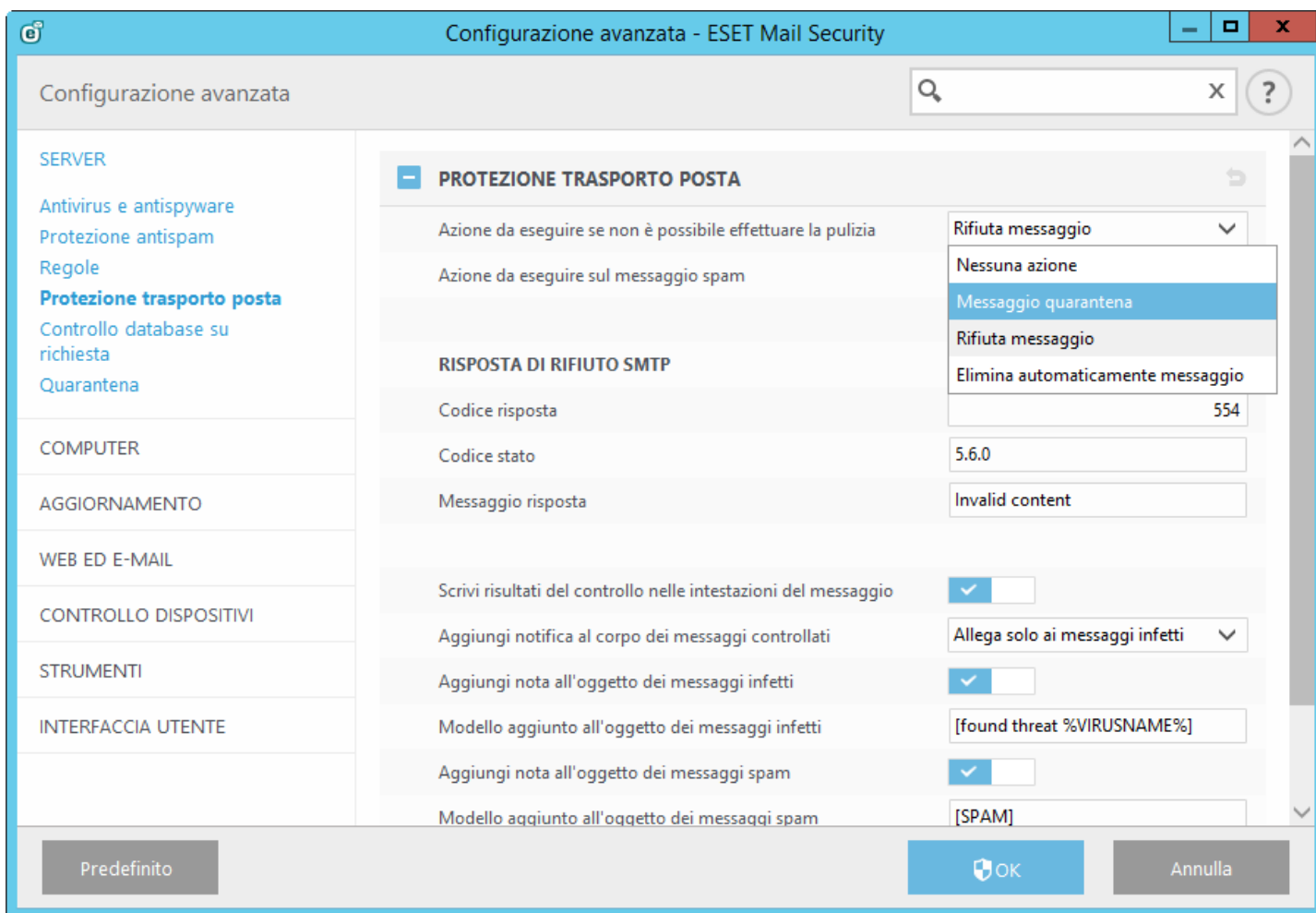
NOTA: i corpi dei messaggi e-mail in formato testo normale non vengono controllati da VSAPI.

NOTA: le cartelle pubbliche vengono trattate allo stesso modo delle caselle di posta. Ciò indica che il controllo viene eseguito anche sulle cartelle pubbliche.

5.1.7 Protezione trasporto posta

Nei seguenti sistemi operativi la **Protezione trasporto posta** è disponibile in **Impostazioni avanzate** > **Server**:

- Microsoft Exchange Server 2007 (server di trasporto Edge o server di trasporto Hub)
- Microsoft Exchange Server 2007 (installazione di server singolo con ruoli multipli)
- Microsoft Exchange Server 2010 (server di trasporto Edge o server di trasporto Hub)
- Microsoft Exchange Server 2010 (installazione di server singolo con ruoli multipli)
- Microsoft Exchange Server 2013 (ruolo di server di trasporto Edge)
- Microsoft Exchange Server 2013 (installazione di server singolo con ruoli multipli)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

Impostazioni protezione trasporto posta:

l'azione antivirus sul livello di trasporto può essere impostata in **Azioni da eseguire se non è possibile effettuare la pulizia:**:

- **Nessuna azione:** mantiene i messaggi infetti che non possono essere puliti
- **Messaggio quarantena:** invia messaggi infetti alla casella di posta della quarantena
- **Rifiuta messaggio:** rifiuta un messaggio infetto
- **Elimina automaticamente messaggio:** elimina i messaggi senza inviare l'NDR (rapporto di mancato recapito)

L'azione antispam sul livello di trasporto può essere impostata in **Azione da eseguire sui messaggi spam**:

- **Nessuna azione**: mantieni il messaggio anche se contrassegnato come spam
- **Messaggio quarantena**: invia i messaggi contrassegnati come spam alla casella di posta della quarantena
- ?**Rifiuta messaggio:** rifiuta messaggi contrassegnati come spam
- **Elimina automaticamente messaggio:** elimina i messaggi senza inviare l'NDR (rapporto di mancato recapito)

Risposta di rifiuto SMTP: è possibile specificare un **Codice risposta**, **Codice stato** e **Messaggio risposta** che definiscono la risposta di rifiuto temporaneo SMTP inviata al server SMTP in caso di rifiuto di un messaggio.

Durante l'eliminazione dei messaggi, invia risposta di rifiuto SMTP:

- Deselezionando l'opzione, il server invia la risposta OK SMTP all'agente di trasferimento messaggi (MTA) del mittente in formato "250 2.5.0: azione e-mail richiesta ok, completata" ed esegue un'eliminazione automatica.
- Selezionando l'opzione, viene rispedita una risposta di rifiuto SMTP all'MTA del mittente. Il messaggio di risposta può essere digitato nei seguenti formati:

Codice risposta primario	Codice stato complementare	Descrizione
250	2.5.0	Azione e-mail richiesta ok, completata

451	4.5.1	Azione richiesta interrotta: errore locale nell'elaborazione
550	5.5.0	Azione richiesta non eseguita: casella di posta non disponibile
554	5.6.0	Contenuto non valido

i **NOTA:** durante la configurazione delle risposte di rifiuto SMTP è anche possibile utilizzare le variabili di sistema.

Aggiungi notifica al corpo dei messaggi controllati offre tre opzioni:
- Non allegare ai messaggi
- Allega solo ai messaggi infetti
- Allega a tutti i messaggi controllati (non vale per i messaggi interni)

Aggiungi nota all'oggetto dei messaggi infetti: attivando l'opzione, ESET Mail Security allegherà un tag di notifica all'oggetto dell'e-mail con il valore definito nel campo testuale **Modello aggiunto all'oggetto dei messaggi spam** (il testo predefinito è [SPAM]). Questa modifica può essere utilizzata per automatizzare il filtraggio antispam attraverso il filtraggio delle e-mail con un oggetto specifico, ad esempio utilizzando regole o, in alternativa, sul lato client (se supportato dal client di posta) allo scopo di inserire tali messaggi e-mail in una cartella separata.

i **NOTA:** durante la modifica del testo che verrà aggiunto all'oggetto è anche possibile utilizzare le variabili di sistema.

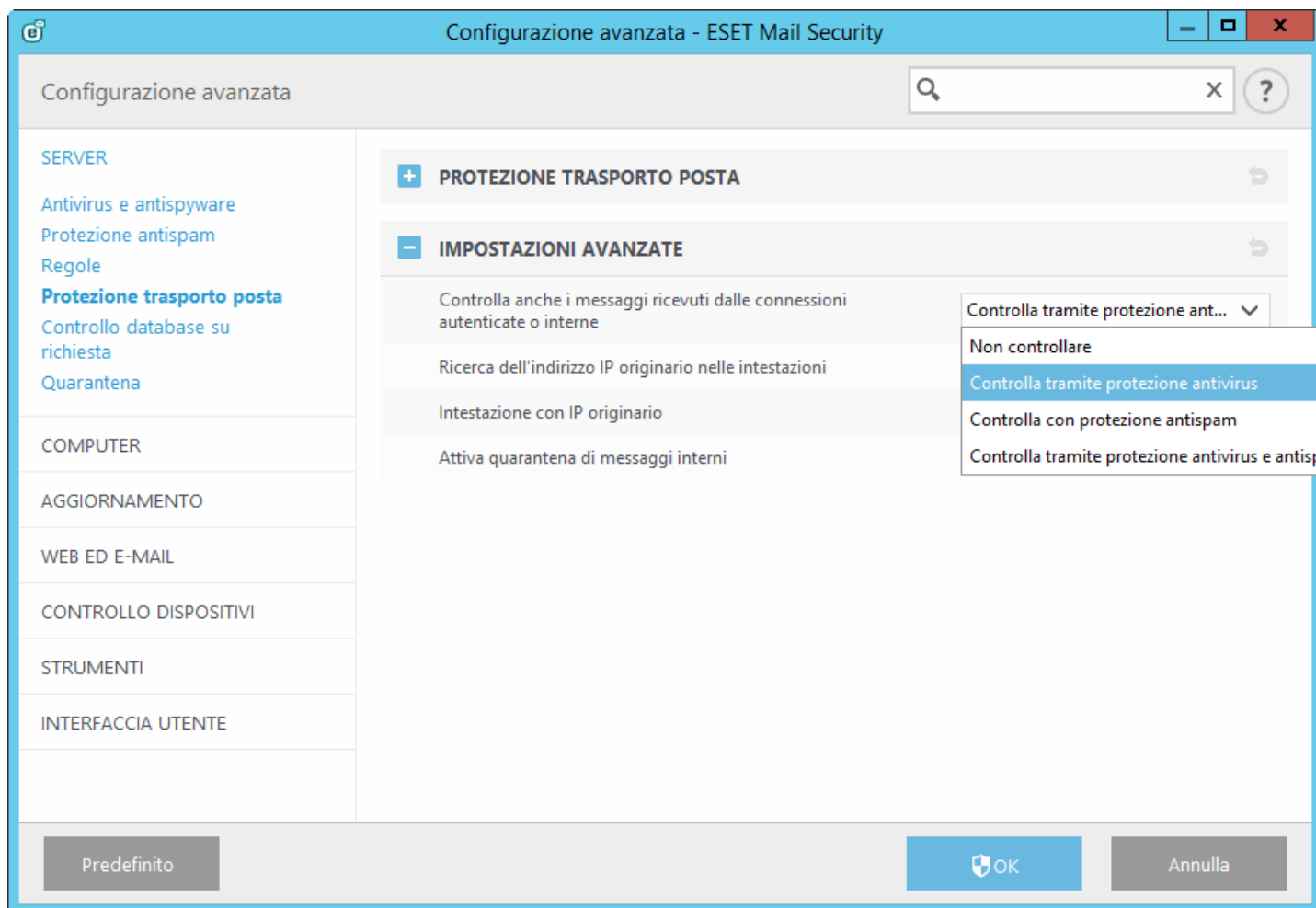
5.1.7.1 Impostazioni avanzate

In questa sezione è possibile modificare le impostazioni avanzate applicate all'agente di trasporto:

- **Controlla anche messaggi ricevuti da connessioni interne o autenticate**: è possibile scegliere il tipo di controllo da eseguire sui messaggi ricevuti da origini autenticate o server locali. Il controllo di questi messaggi è consigliato poiché aumenta il livello di protezione. Inoltre, se si utilizza il connettore POP3 integrato Microsoft SBS per recuperare i messaggi e-mail da server POP3 esterni o servizi di posta elettronica, come **Gmail.com**, **Outlook.com**, **Yahoo.com**, **gmx.dem** e altri ancora, tale controllo diventa addirittura necessario. Per ulteriori informazioni, consultare Connettore POP3 e antispam.

- **Ricerca dell'indirizzo IP originario nelle intestazioni**: se questa opzione è attivata, ESET Mail Security cerca gli indirizzi IP originari nelle intestazioni dei messaggi affinché possano essere utilizzati da diversi moduli di protezione (antispam e altri). Se l'azienda che utilizza Exchange è separata da Internet mediante un proxy, un gateway o server Trasporto Edge, i messaggi e-mail sembrano arrivare da un unico indirizzo IP (generalmente uno interno). Di solito, sul server esterno (ad esempio, il server Trasporto Edge in DMZ) in cui l'indirizzo IP dei mittenti è noto, tale indirizzo viene scritto nelle intestazioni del messaggio e-mail ricevuto. Il valore immesso nel campo **Intestazione con IP originario** seguente rappresenta l'intestazione che ESET Mail Security cerca nelle intestazioni dei messaggi.

- **Intestazione con IP originario**: è l'intestazione che ESET Mail Security cerca nelle intestazioni dei messaggi. L'impostazione predefinita è **IP-originario-X**, ma se si utilizzano strumenti forniti da terze parti o personalizzati che sono contraddistinti da un tipo di intestazione diversa, sarà necessario cambiare l'impostazione con una più appropriata.

- **Attiva quarantena di messaggi interni**: quando questa opzione è attivata, i messaggi interni vengono messi in quarantena.

5.1.8 Controllo database su richiesta

Elenco di sistemi per i quali è disponibile il **Controllo database su richiesta**:

- Microsoft Exchange Server 2007 (server della casella di posta o server di trasporto Hub)
- Microsoft Exchange Server 2007 (installazione di server singolo con ruoli multipli)
- Microsoft Exchange Server 2010 (server della casella di posta o server di trasporto Hub)
- Microsoft Exchange Server 2010 (installazione di server singolo con ruoli multipli)
- Microsoft Exchange Server 2013 (ruolo del server della casella di posta)
- Microsoft Exchange Server 2013 (installazione di server singolo con ruoli multipli)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

NOTA: in caso di esecuzione di Microsoft Exchange Server 2007 o 2010, è possibile scegliere tra la Protezione database casella di posta e il Controllo database su richiesta. Tuttavia, è possibile attivare esclusivamente uno dei due tipi di protezione alla volta. Se si decide di utilizzare il controllo database su richiesta, sarà necessario disattivare l'integrazione della protezione database casella di posta nella Configurazione avanzata in Server. In caso contrario, il Controllo database su richiesta non sarà disponibile.

Impostazioni controllo database su richiesta:

Indirizzo host: nome o indirizzo IP del server che esegue EWS (Exchange Web Services).

Nome utente: specificare le credenziali di un utente che ha correttamente accesso a EWS (Exchange Web Services).

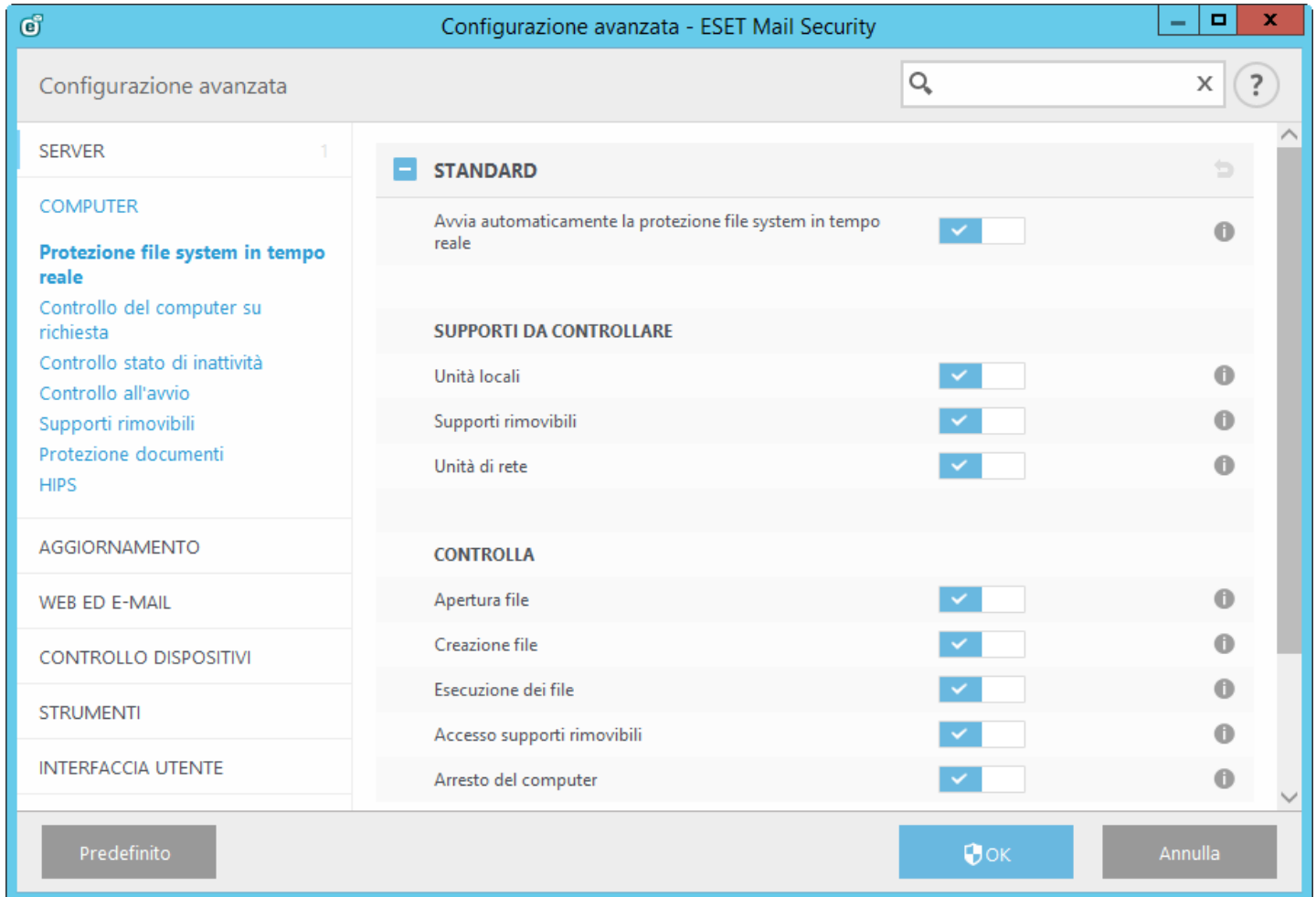
Password utente: fare clic su **Imposta** accanto a **Password utente** e digitare la password per questo account utente.

Assegna ruolo ApplicationImpersonation all'utente: fare clic su **Assegna** per assegnare automaticamente il ruolo ApplicationImpersonation all'utente selezionato.

Utilizza SSL: è necessario abilitare questa opzione se EWS (Exchange Web Services) è impostato su **Richiedi SSL** in

IIS. Se SSL è attivato, il certificato di Exchange Server deve essere importato sul sistema con ESET Mail Security (nel caso in cui i ruoli di Exchange Server si trovino su server diversi). Le impostazioni di EWS sono disponibili in IIS in *Siti/Sito Web predefinito/EWS/Impostazioni SSL*.

i **NOTA**: disattivare **Utilizza SSL** solo se EWS è stato configurato in IIS in modo da non richiedere l'SSL.

Certificato del client: deve essere impostato esclusivamente se richiesto da Exchange Web Services. **Seleziona** consente all'utente di selezionare un qualsiasi certificato.

Azione da eseguire se non è possibile effettuare la pulizia: questo campo di azioni consente all'utente di **bloccare** i contenuti infetti.

Nessuna azione: non esegue alcuna azione sul contenuto infetto del messaggio.
Sposta messaggio nel cestino: non è supportato per gli oggetti delle cartelle pubbliche. L'opzione **Elimina oggetto** consente invece di applicare l'azione.
Elimina oggetto: contenuto infetto del messaggio.
Elimina messaggio: elimina l'intero messaggio compresi i contenuti infetti.
Sostituisci oggetto con informazioni sull'azione: rimuove un oggetto e inserisce le informazioni relative all'azione intrapresa con questo oggetto.

5.1.8.1 Voci aggiuntive casella di posta

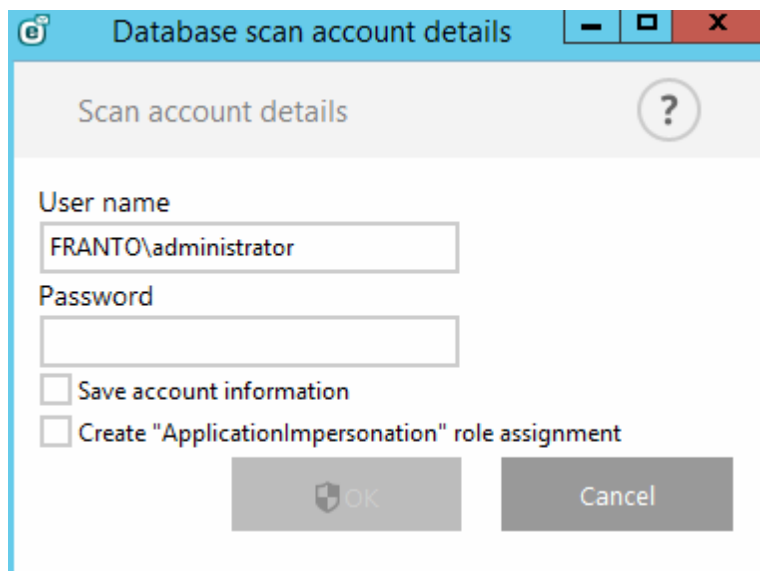
Le impostazioni del controllo del database su richiesta consentono all'utente di attivare o disattivare il controllo di altri tipi di oggetti della casella di posta:

- Controlla calendario
- Controlla attività
- Controlla contatti
- Controlla diario

i **NOTA:** in caso di problemi relativi alle prestazioni, è possibile disattivare il controllo di questi oggetti. In caso di attivazione di questi oggetti, i controlli avranno una durata maggiore.

5.1.8.2 Server proxy

In caso di utilizzo di un server proxy tra Exchange Server con il ruolo CAS e Exchange Server su cui è installato ESET Mail Security, è necessario specificare i parametri del server proxy. Tale azione è obbligatoria in quanto ESET Mail Security effettua la connessione all'API di EWS (Exchange Web Services) mediante HTTP/HTTPS. In caso contrario, il controllo database su richiesta non funzionerà.

Server proxy: inserire l'indirizzo IP o il nome del server proxy utilizzato.

Porta: inserire il numero della porta del server proxy.

Nome utente, password: inserire le credenziali se il server proxy richiede l'autenticazione.

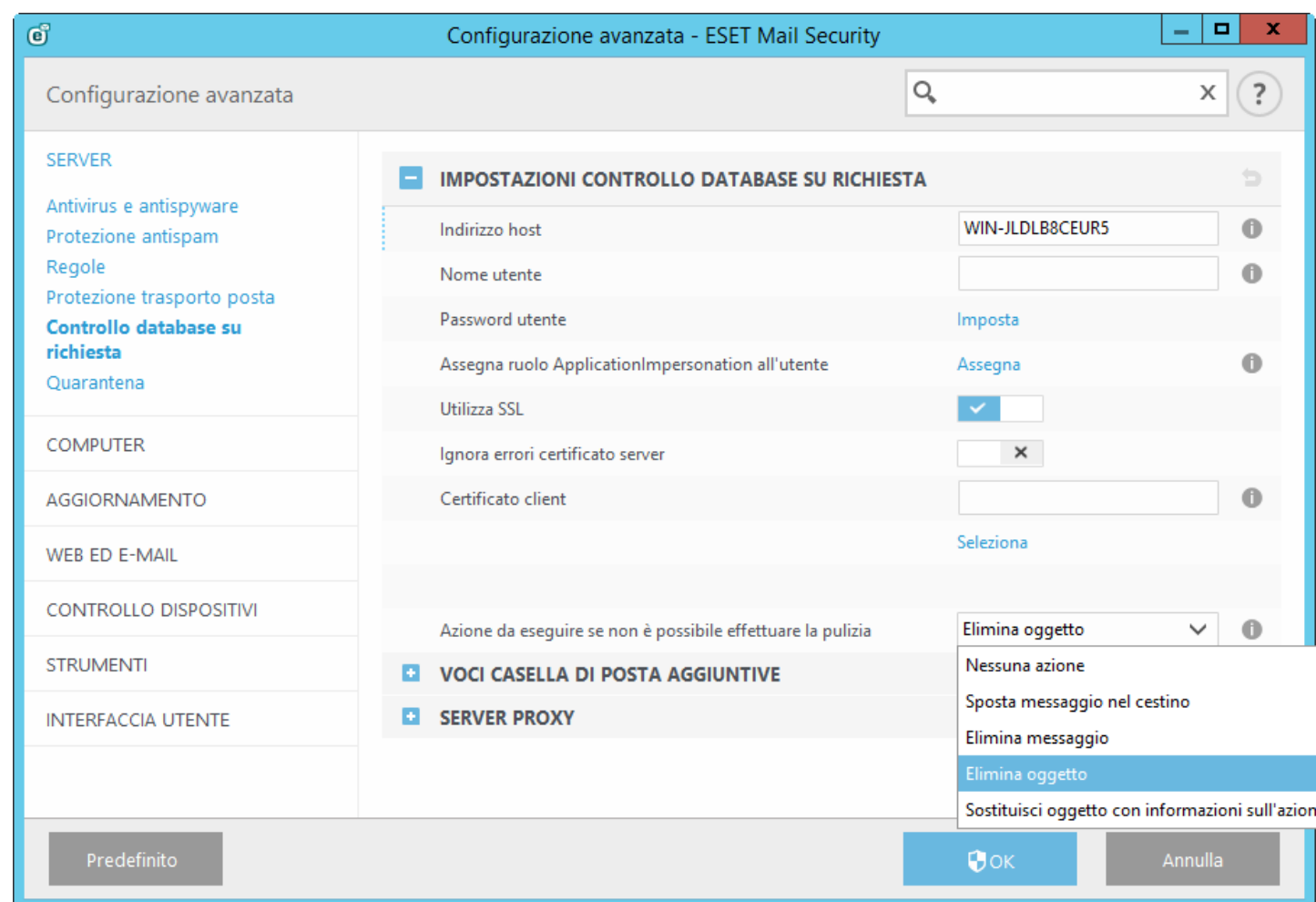
5.1.8.3 Dettagli account controllo database

Questa finestra di dialogo viene visualizzata se l'utente non ha specificato un nome utente e una password per il **Controllo database** in **Configurazione avanzata**. Specificare le credenziali dell'utente che ha accesso a EWS (Exchange Web Services) in questa finestra popup e fare clic su **OK**. In alternativa, accedere a **Configurazione avanzata** premendo **F5** e a **Server** > Controllo database su richiesta. Digitare il **Nome utente**, fare clic su **Imposta**, digitare una password per l'account utente e fare clic su OK.

- È possibile selezionare **Salva informazioni account** per salvare le impostazioni dell'account, per evitare di doverle inserire a ogni esecuzione di un controllo del database su richiesta.
- Se un account utente non possiede un accesso appropriato a EWS, è possibile selezionare **Crea l'assegnazione del ruolo "ApplicationImpersonation"** per assegnare il ruolo a un account.

5.1.9 Quarantena delle e-mail

La gestione quarantena e-mail è disponibile per tutti e tre i tipi di quarantena:

- Quarantena locale
- Casella di posta della quarantena
- Quarantena di MS Exchange

È possibile visualizzare i contenuti della quarantena delle e-mail in Gestione quarantena e-mail per tutti i tipi di quarantena. È inoltre possibile visualizzare la quarantena locale nell'Interfaccia Web della quarantena delle e-mail.

5.1.9.1 Quarantena locale

La quarantena locale utilizza il file system locale per archiviare le mail in quarantena e un database SQLite come indice. I file delle e-mail in quarantena archiviate e il file del database sono crittografati per motivi di sicurezza. Questi file si trovano in `C:\ProgramData\ESET\ESET Mail Security\MailQuarantine` (su Windows Server 2008 e 2012) o `C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\MailQuarantine` (su Windows Server 2003).

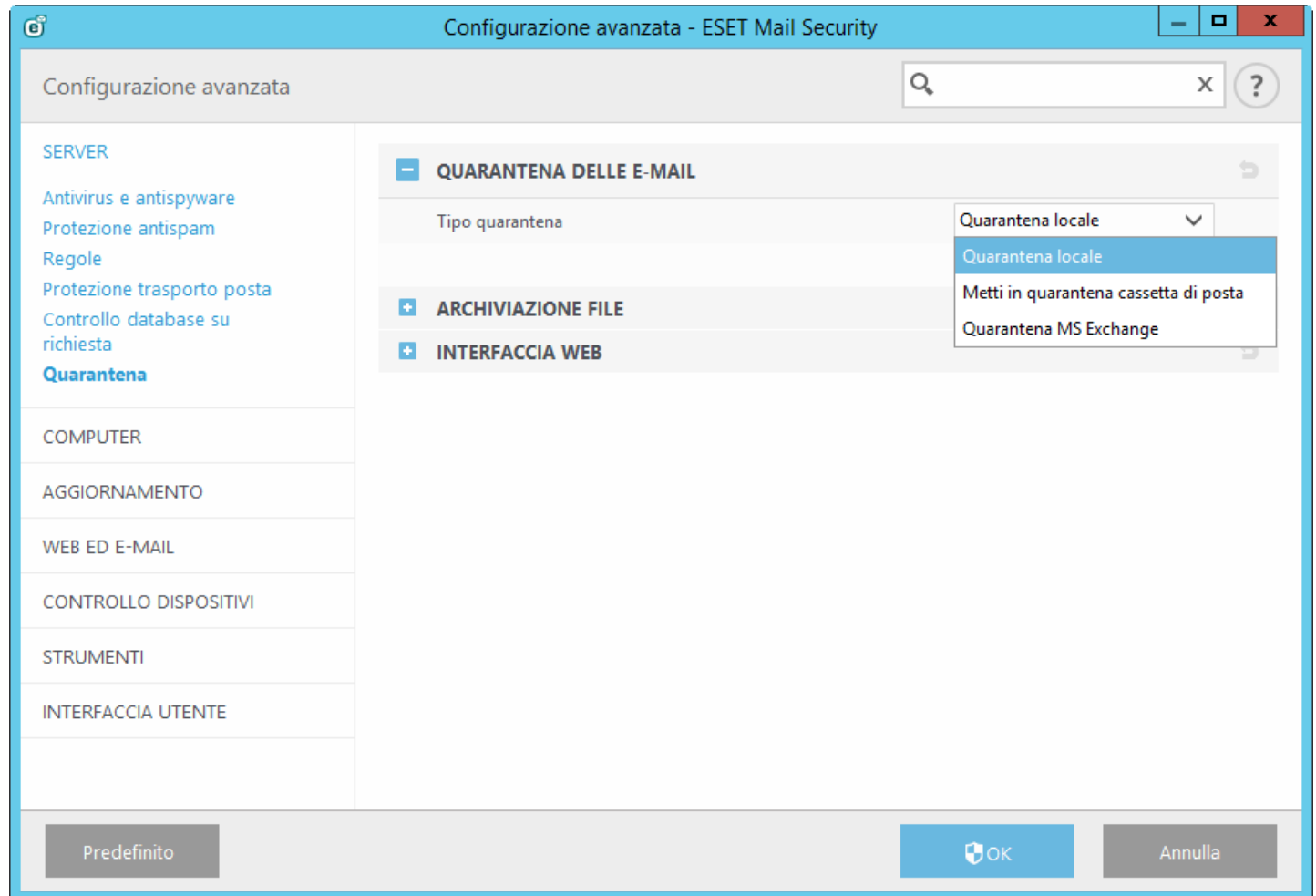
Funzioni quarantena locale:

- Crittografia e compressione dei file delle e-mail in quarantena archiviate.
- I file delle e-mail in quarantena rimosse dalla finestra della quarantena (per impostazione predefinita dopo 21 giorni), sono ancora archiviati in un file system (finché non verrà eseguita un'eliminazione automatica dopo un numero di giorni specifico)
- Eliminazione automatica dei file di vecchie e-mail (per impostazione predefinita dopo 3 giorni). Per maggiori informazioni, consultare Impostazioni archiviazione file.
- I file delle e-mail in quarantena rimosse possono essere ripristinati mediante eShell (ipotizzando che non siano ancora stati eliminati dal file system).

È possibile ispezionare i messaggi e-mail in quarantena e decidere di **eliminarli** o **rilasciarli**. Per visualizzare e

gestire localmente i messaggi e-mail in quarantena, è possibile utilizzare la Gestione quarantena e-mail nella GUI principale o l'interfaccia Web della quarantena delle e-mail.

5.1.9.1.1 Archiviazione file

In questa sezione è possibile modificare le impostazioni per l'archiviazione dei file utilizzate dalla quarantena locale.

Comprimi file in quarantena: i file in quarantena compressi occupano una minore quantità di spazio sul disco. Tuttavia, se si decide di non avere file compressi, utilizzare il pulsante per disattivare la compressione.

Cancella vecchi file dopo (giorni): dopo un numero specifico di giorni, i messaggi vengono rimossi dalla finestra della quarantena. Tuttavia, i file non verranno eliminati dal disco per il numero di giorni specificato in **Cancella file eliminati dopo (giorni)**. Poiché i file non vengono eliminati dal file system, è possibile recuperarli utilizzando eShell.

Cancella file eliminati dopo (giorni): elimina i file dal disco dopo il numero di giorni specificato. In seguito a questa eliminazione, non sarà possibile eseguire alcuna operazione di recupero (a meno che non sia stata attuata una soluzione di backup del file system).

Archivia messaggi per destinatari inesistenti: solitamente i messaggi spam vengono inviati a destinatari casuali per un dato dominio nel tentativo di colpirne uno esistente. I messaggi inviati a utenti non presenti in una Active Directory vengono archiviati nella quarantena locale per impostazione predefinita. Tuttavia, disattivando questa funzione, i messaggi inviati ai destinatari inesistenti non verranno archiviati. In tal modo, la quarantena locale non sarà inondata da un numero eccessivo di messaggi spam di questo tipo. Questa opzione consente anche di risparmiare spazio sul disco.

5.1.9.1.2 Interfaccia Web

L'interfaccia Web della quarantena delle e-mail è un'alternativa alla Gestione quarantena e-mail. Tuttavia, è disponibile esclusivamente per la Quarantena locale.

NOTA: l'interfaccia Web della quarantena delle e-mail non è disponibile su un server dotato del ruolo di server Trasporto Edge, in quanto non è possibile accedere ad Active Directory per l'autenticazione.

L'interfaccia Web della quarantena delle e-mail consente all'utente di visualizzare lo stato della quarantena delle e-mail, nonché di gestire gli oggetti delle e-mail in quarantena. L'interfaccia Web è accessibile mediante collegamenti presenti nei report della quarantena o direttamente mediante l'inserimento di un URL nel browser Web. Per accedere all'interfaccia Web della quarantena delle e-mail, è necessario effettuare l'autenticazione mediante l'utilizzo delle credenziali del dominio. Internet Explorer effettuerà l'autenticazione automatica per un utente del dominio, il certificato della pagina Web deve essere valido, in IE è necessario attivare l'Accesso automatico ed è necessario aggiungere il sito Web della quarantena delle e-mail tra i siti Intranet locali.

Il pulsante **Attiva interfaccia Web** consente all'utente di disattivare o attivare l'interfaccia Web.

Rilascia: rilascia l'e-mail a uno o più destinatari originali utilizzando la directory Rispondi e la elimina dalla quarantena. Fare clic su **Invia** per confermare l'azione.
Elimina: elimina l'oggetto dalla quarantena. Fare clic su **Invia** per confermare l'azione.

Facendo clic su **Oggetto**, si aprirà una finestra popup contenente i dettagli dell'e-mail in quarantena, come ad esempio il **Tipo**, il **Motivo**, il **Mittente**, la **Data**, gli **Allegati**, ecc.

Fare clic su **Mostra intestazioni** per rivedere l'intestazione dell'oggetto in quarantena.

Quarantined mail detail

TYPE	spam
REASON	Found GTUBE test string
SUBJECT	hlavicka
SENDER	test@test.sk
SMTP RECIPIENTS	vista@s2.local
TO	vista@s2.local
CC	
DATE	2015-06-22 23:28
ATTACHMENTS	

```
Received: from win2k3r2x64-ss4 ([10.1.117.232]) by win2k3sp2x86ss1.s2.local with Microsoft SMTPSVC(6.0.3790.4675);
        Mon, 22 Jun 2015 23:28:46 -0700
Received:
To: <vista@s2.local>
Subject:[SPAM] hlavicka
X-Originating-IP:
MIME-Version: 1.0
Content-Type: text/plain
Message-ID: <-974233353.8808@win2k8x64-EDGE.s1.local>
From:
Return-Path: < >
Date: Tue, 9 Nov 2010 22:12:48 -0800
X-MS-Exchange-Organization-OriginalArrivalTime: 10 Nov 2010 06:12:48.9975
 (UTC)
X-MS-Exchange-Organization-AuthSource: win2k8x64-EDGE.s1.local
X-MS-Exchange-Organization-AuthAs: Anonymous
Received-SPF: Fail (win2k8x64-EDGE.s1.local: domain of  does not designate
 10.1.117.225 as permitted sender) receiver=win2k8x64-EDGE.s1.local;
```

RELEASE DELETE Go to quarantine view.

Se lo si desidera, fare clic su **Rilascia**o **Elimina** per eseguire un'azione con un messaggio e-mail in quarantena.

ℹ **NOTA**: per uscire completamente dall'interfaccia Web della quarantena delle e-mail è necessario chiudere la finestra del browser. In alternativa, fare clic su **Vai** per accedere alla visualizzazione della quarantena e ritornare alla schermata precedente.

Importante: in caso di problemi di accesso all'interfaccia Web della quarantena delle e-mail dal browser in uso o di comparsa dell'errore `HTTP 403.4 - Vietato` o un errore simile, verificare il Tipo di quarantena selezionato e assicurarsi che si tratti della **Quarantena locale** e che **Attiva interfaccia Web** sia attivato.

5.1.9.2 Casella di posta della quarantena e quarantena di MS Exchange

Se si decide di non utilizzare la Quarantena locale, sono disponibili due opzioni, vale a dire la **Casella di posta della quarantena** o la **Quarantena di MS Exchange**. Indipendentemente dall'opzione scelta, è necessario creare un utente dedicato con la casella di posta (ad esempio, quarantena_principale@azienda.com) che verrà utilizzato per archiviare i messaggi e-mail in quarantena. Questo utente e la casella di posta verranno utilizzati anche dalla Gestione quarantena e-mail per visualizzare e gestire gli oggetti presenti nella quarantena. Sarà necessario specificare i dettagli dell'account di questo utente nelle Impostazioni della gestione quarantena.

Importante: si sconsiglia di utilizzare l'account utente Amministratore come casella di posta della quarantena.

NOTA: la **Quarantena di MS Exchange** non è disponibile per Microsoft Exchange 2003, ma solo la **Quarantena locale** e la **Casella di posta della quarantina**.

- Selezionando la **Quarantena di MS Exchange**, ESET Mail Security utilizzerà il **Sistema di quarantena di Microsoft Exchange** (ciò vale per Microsoft Exchange Server 2007 e versioni successive). In tal caso, il meccanismo interno di Exchange viene utilizzato per l'archiviazione di messaggi potenzialmente infetti e SPAM.

NOTA: per impostazione predefinita, la quarantena interna non è attivata in Exchange. Per attivarla, è necessario aprire Exchange Management Shell e digitare il seguente commando (sostituire `nome@dominio.com` con l'indirizzo effettivo della casella di posta dedicata):

```
Set-ContentFilterConfig -QuarantineMailbox nome@dominio.com
```

- Se si seleziona **Casella di posta della quarantena**, è necessario specificare l'indirizzo della quarantena del messaggio (ad esempio quarantena_principale@azienda.com).

5.1.9.2.1 Impostazioni gestione quarantena

Indirizzo host: comparirà automaticamente se localmente è presente Exchange Server con il ruolo CAS. In alternativa, se il ruolo CAS non è presente nello stesso server su cui è installato ESET Mail Security, ma può essere trovato all'interno di AD, l'indirizzo host comparirà automaticamente. In caso contrario, è possibile digitare il nome host manualmente. L'eliminazione automatica non funzionerà con il ruolo del server di trasporto Edge.

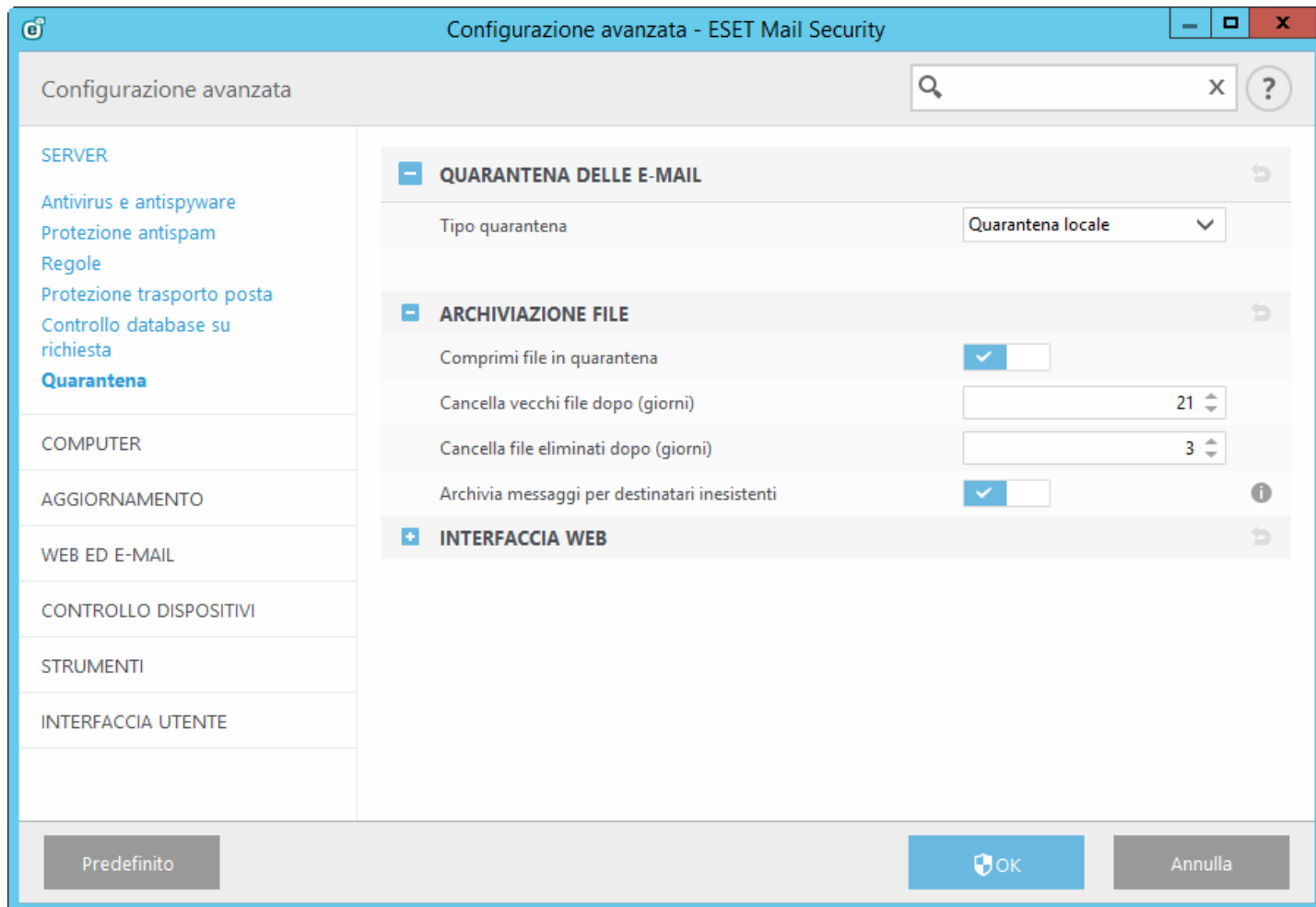
NOTA: poiché l'indirizzo IP non è supportato, è necessario utilizzare il nome host del server CAS.

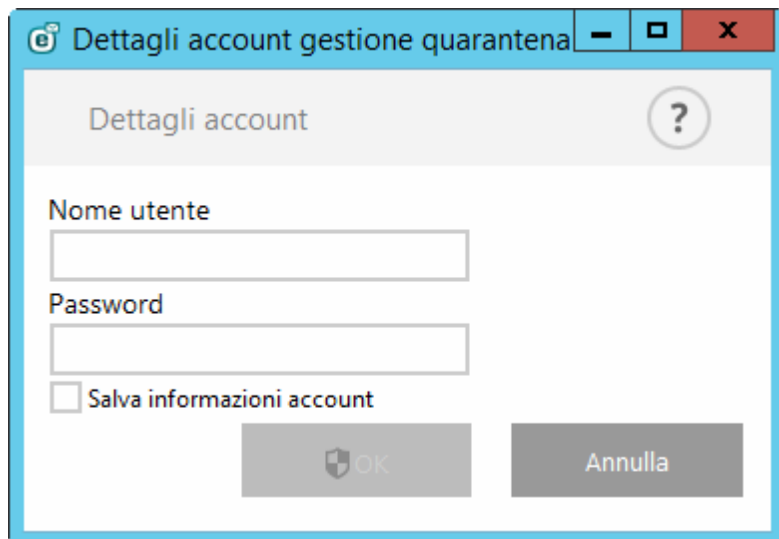
Nome utente: account utente della quarantena dedicato creato per l'archiviazione di messaggi in quarantena (o un account che ha accesso a questa casella di posta attraverso la delega di accesso). Sul ruolo del server di trasporto Edge che non fa parte del dominio è necessario utilizzare l'intero indirizzo e-mail (ad esempio quarantena_principale@azienda.com).

Password: digitare la password dell'account della quarantena.

Utilizza SSL: è necessario abilitare questa opzione se EWS (Exchange Web Services) è impostato su **Richiedi SSL** in IIS. Se SSL è attivato, il certificato di Exchange Server deve essere importato sul sistema con ESET Mail Security (nel caso in cui i ruoli di Exchange Server si trovino su server diversi). Le impostazioni di EWS sono disponibili in IIS in *Siti/Sito Web predefinito/EWS/Impostazioni SSL*.

NOTA: disattivare **Utilizza SSL** solo se EWS è stato configurato in IIS in modo da non richiedere l'SSL.

Ignora errori certificato server: ignora i seguenti stati: autofirmato, nome errato nel certificato, utilizzo errato, scaduto.

5.1.9.2.2 Server proxy

In caso di utilizzo di un server proxy tra Exchange Server con il ruolo CAS e Exchange Server su cui è installato ESET Mail Security, è necessario specificare i parametri del server proxy. Tale azione è obbligatoria in quanto ESET Mail Security effettua la connessione all'API di EWS (Exchange Web Services) mediante HTTP/HTTPS. In caso contrario, la casella di posta della quarantena e la quarantena di MS Exchange non funzioneranno.

Server proxy: inserire l'indirizzo IP o il nome del server proxy utilizzato.

Porta: inserire il numero della porta del server proxy.

Nome utente, password: inserire le credenziali se il server proxy richiede l'autenticazione.

5.1.9.3 Dettagli account gestione quarantena

La finestra di dialogo verrà visualizzata in caso di mancata configurazione di un account per i **Dettagli account gestione quarantena**. Specificare le credenziali di un utente con accesso alla **Casella di posta della quarantena** e fare clic su **OK**. In alternativa, premere F5 per accedere alla **Configurazione avanzata** e a **Server** > **Quarantena e-mail** > Impostazioni gestione quarantena. Digitare il **Nome utente** e la **Password** per la casella di posta della quarantena.

È possibile selezionare **Salva informazioni account** per salvare le impostazioni dell'account per utilizzi futuri in caso di accesso alla gestione quarantena.

5.1.10 Cluster

ESET Cluster è un'infrastruttura di comunicazione P2P della gamma di prodotti ESET per Microsoft Windows Server.

Questa infrastruttura consente ai prodotti server ESET di comunicare tra loro e scambiare dati quali configurazioni e notifiche, oltre a sincronizzare i dati necessari per il corretto funzionamento di un gruppo di istanze del prodotto. Un esempio potrebbe essere un gruppo di nodi in un cluster di failover Windows o cluster NLB (Network Load Balancing) con il prodotto ESET installato dove è richiesta la stessa configurazione del prodotto sull'intero cluster. ESET Cluster assicura questo livello di coerenza tra le istanze.

La pagina di stato di ESET Cluster è accessibile dal menu principale in **Strumenti** > **Cluster** (se configurato correttamente) e presenta le seguenti caratteristiche:

Per configurare ESET Cluster, fare clic su **Procedura guidata cluster...** Per informazioni dettagliate sulle modalità di configurazione di ESET Cluster tramite la procedura guidata, fare clic qui.

Per configurare ESET Cluster, sono disponibili due metodi di aggiunta dei nodi: in maniera automatica, attraverso l'utilizzo del cluster di failover Windows/cluster NLB esistente, o manualmente, attraverso la ricerca dei computer presenti in un gruppo di lavoro o dominio.

Rilevamento automatico: rileva automaticamente i nodi che sono già membri di un cluster di failover Windows/ cluster NLB e li aggiunge a ESET Cluster
Sfoglia: è possibile aggiungere manualmente i nodi digitando i nomi del server (membri dello stesso gruppo di lavoro o membri dello stesso dominio)

NOTA: non è necessario che i server siano membri di un cluster di failover Windows/cluster NLB per poter utilizzare la funzione ESET Cluster. Per l'utilizzo dei cluster ESET nel proprio ambiente di lavoro, non è necessario un cluster di failover Windows/cluster NLB.

Dopo aver aggiunto i nodi a ESET Cluster, è necessario installare ESET Mail Security su ciascuno di essi. Questa operazione viene eseguita automaticamente durante la configurazione di ESET Cluster.

Le credenziali richieste per l'installazione remota di ESET Mail Security su altri nodi cluster sono le seguenti:

- Scenario dominio: credenziali amministratore del dominio
- Scenario gruppo di lavoro: è necessario accertarsi che tutti i nodi utilizzino le stesse credenziali dell'account amministratore locale

In ESET Cluster è inoltre possibile utilizzare una combinazione di nodi aggiunti automaticamente come membri di un cluster di failover Windows/cluster NLB esistente e di nodi aggiunti manualmente (a condizione che si trovino nello stesso dominio).

NOTA: non è possibile associare nodi del dominio a nodi del gruppo di lavoro.

Un altro requisito per l'utilizzo di ESET Cluster consiste nel fatto che l'opzione **Condivisione file e stampanti** sia attiva in Windows Firewall prima dell'avvio dell'installazione di ESET Mail Security sui nodi di ESET Cluster.

ESET Cluster può essere facilmente eliminato facendo clic su **Elimina cluster**. Ciascun nodo scriverà un record nel relativo rapporto eventi sull'ESET Cluster eliminato. Successivamente, tutte le regole del firewall ESET verranno rimosse da Windows Firewall. I primi nodi ritorneranno quindi nello stato precedente e potranno essere nuovamente utilizzati in un altro ESET Cluster, se necessario.

NOTA: la creazione di ESET Cluster tra ESET Mail Security ed ESET File Security for Linux non è supportata.

In qualsiasi momento, è possibile aggiungere nuovi nodi a un ESET Cluster esistente eseguendo la **Procedura guidata cluster** in base alle modalità descritte in precedenza e qui.

Per ulteriori informazioni sulla configurazione di ESET Cluster, consultare la sezione Cluster di lavoro.

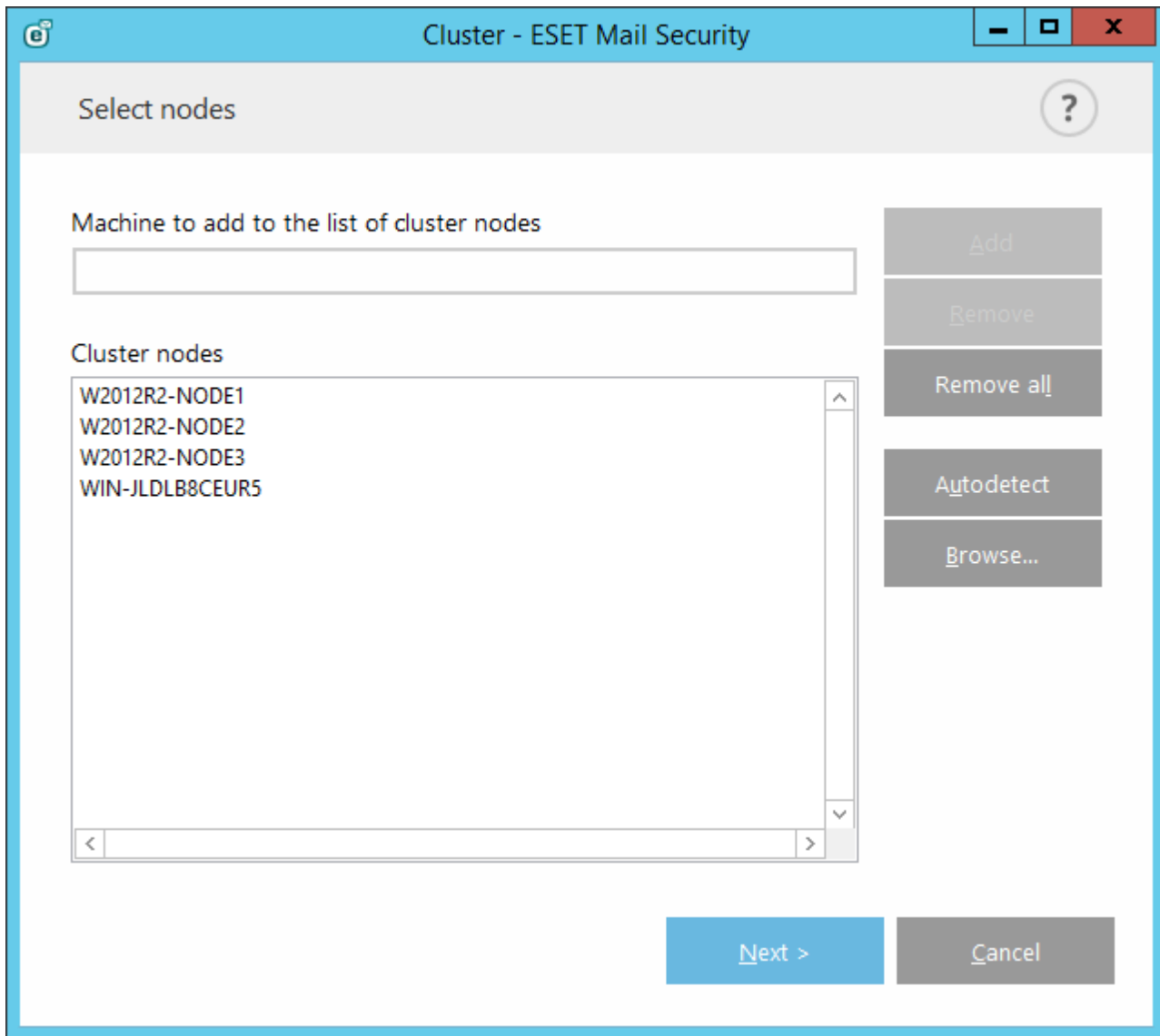
5.1.10.1 Procedura guidata cluster: pagina 1

La prima operazione da eseguire per configurare ESET Cluster consiste nell'aggiunta di nodi. Per aggiungere nodi, è possibile utilizzare l'opzione **Rilevamento automatico** oppure **Sfoglia**. In alternativa, è possibile digitare il nome del server nella casella di testo e fare clic sul pulsante **Aggiungi**.

L'opzione **Rilevamento automatico** consente di aggiungere automaticamente nodi da un cluster di failover Windows/cluster NLB (Network Load Balancing) esistente. Per poter aggiungere automaticamente nodi, il server in uso per la creazione di ESET Cluster deve essere un membro di questo cluster di failover Windows/cluster NLB (Network Load Balancing). Affinché ESET Cluster possa rilevare correttamente i nodi, è necessario che nelle proprietà del cluster NLB sia attiva la funzionalità **Consenti controllo remoto**. Una volta visualizzato l'elenco dei nodi aggiunti di recente, è possibile rimuovere quelli indesiderati, nel caso in cui si desideri che ESET Cluster contenga solo nodi specifici.

Fare clic su **Sfoglia** per trovare e selezionare i computer all'interno di un dominio o di un gruppo di lavoro. Questo metodo consente di aggiungere manualmente nodi a ESET Cluster.

Per aggiungere nodi è anche possibile digitare il nome host del server che si desidera aggiungere e fare clic su **Aggiungi**.

Nodi cluster correnti scelti per essere aggiunti a ESET Cluster dopo aver fatto clic su **Avanti**:

Per modificare i **Nodi cluster** nell'elenco, selezionare il nodo che si desidera rimuovere e fare clic su **Rimuovi** oppure fare clic su **Rimuovi tutto** per cancellare completamente l'elenco.

Nel caso in cui si disponesse già di ESET Cluster esistente, è possibile aggiungere nuovi nodi in qualsiasi momento. Le operazioni da eseguire sono identiche a quelle descritte in precedenza.

NOTA: tutti i nodi che rimangono nell'elenco devono essere on-line e raggiungibili. L'host locale viene aggiunto ai nodi cluster per impostazione predefinita.

5.1.10.2 Procedura guidata cluster: pagina 2

Definire il nome del cluster e la modalità di distribuzione del certificato e decidere se installare o meno il prodotto sugli altri nodi.

Nome cluster: digitare il nome del cluster.
Porta di ascolto (la porta predefinita è 9777)
Apri porta in Windows Firewall: se selezionata, viene creata una regola in Windows Firewall.

Distribuzione certificato:
Remota automatica: il certificato verrà installato automaticamente.
Manuale: quando si fa clic su **Genera**, si aprirà una finestra Sfoglia in cui bisognerà selezionare la cartella dove archiviare i certificati. Verrà creato un certificato radice, nonché un certificato per ciascun nodo, compreso quello (macchina locale) dal quale si sta configurando ESET Cluster. È quindi possibile scegliere di registrare il certificato sul computer locale facendo clic su **Sì**. Più avanti sarà necessario importare i certificati manualmente come descritto qui.

Installazione prodotto su altri nodi:
Remota automatica: ESET Mail Security verrà installato automaticamente su ciascun nodo (a condizione che i relativi sistemi operativi abbiano la stessa architettura).
Manuale: scegliere questa opzione per installare ESET Mail Security manualmente (ad esempio, quando su alcuni nodi sono presenti architetture di sistemi operativi differenti).

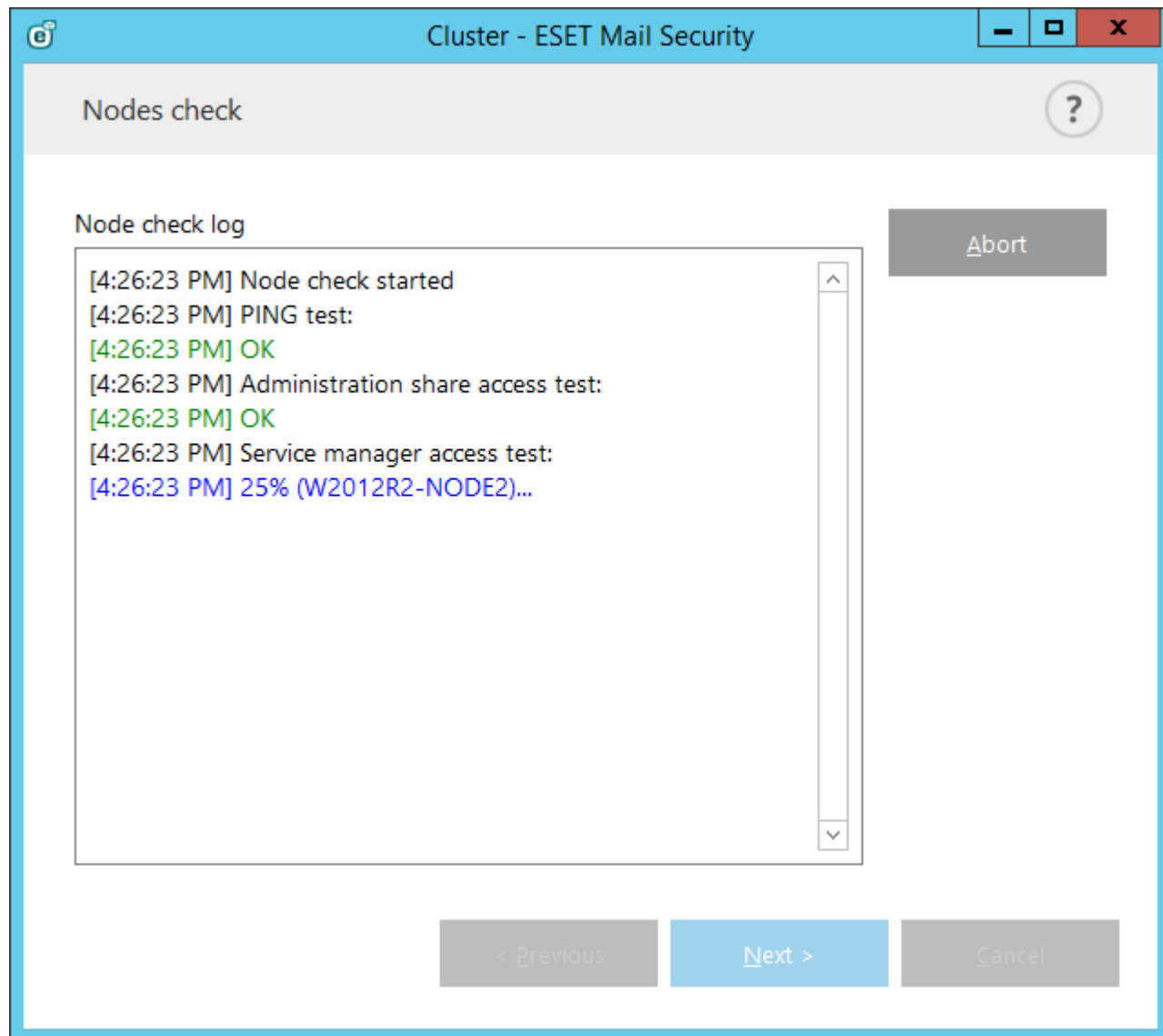
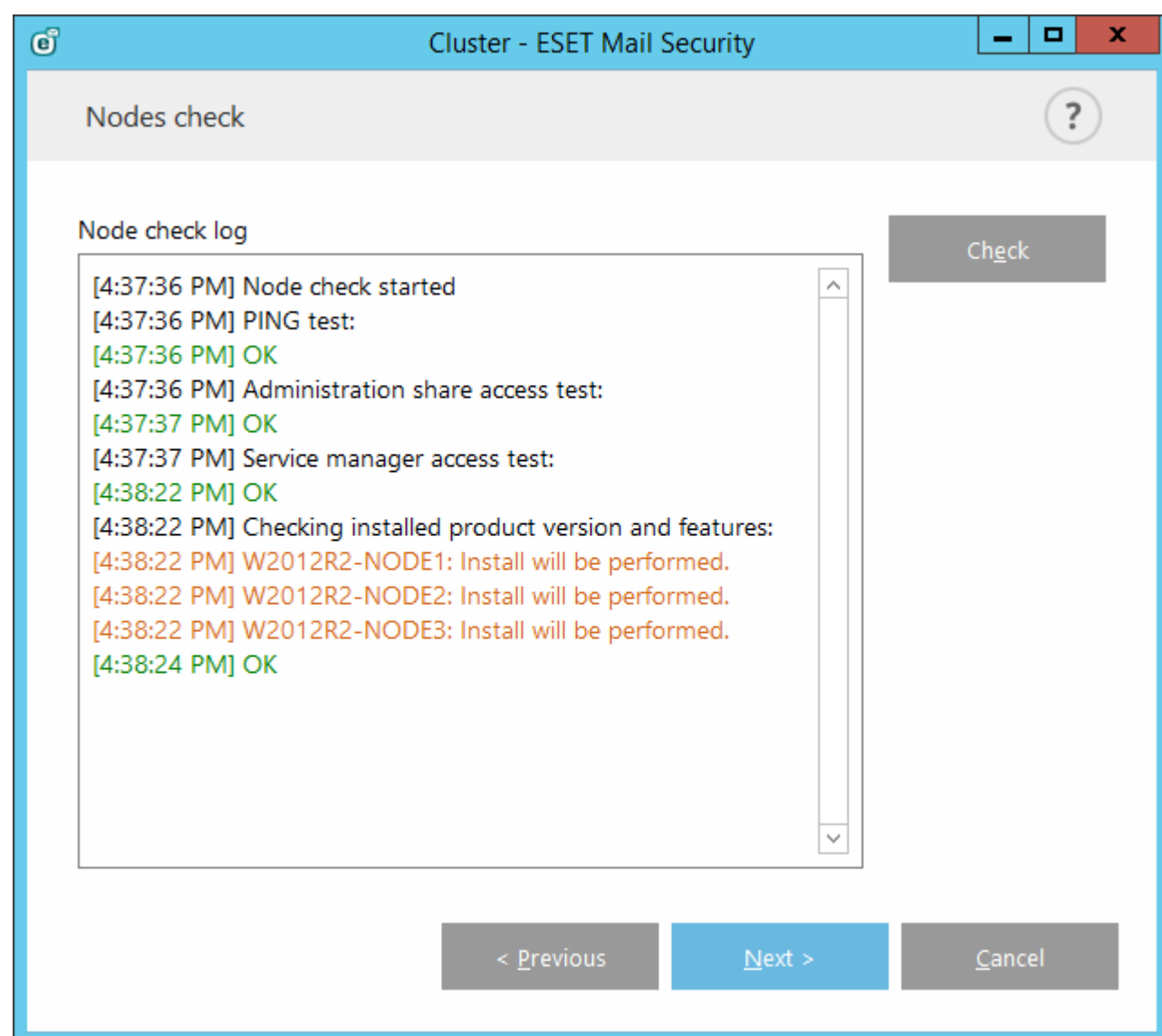
Esegui il push della licenza sui nodi senza prodotto attivato: selezionando questa opzione, i nodi attiveranno ESET Mail Security.

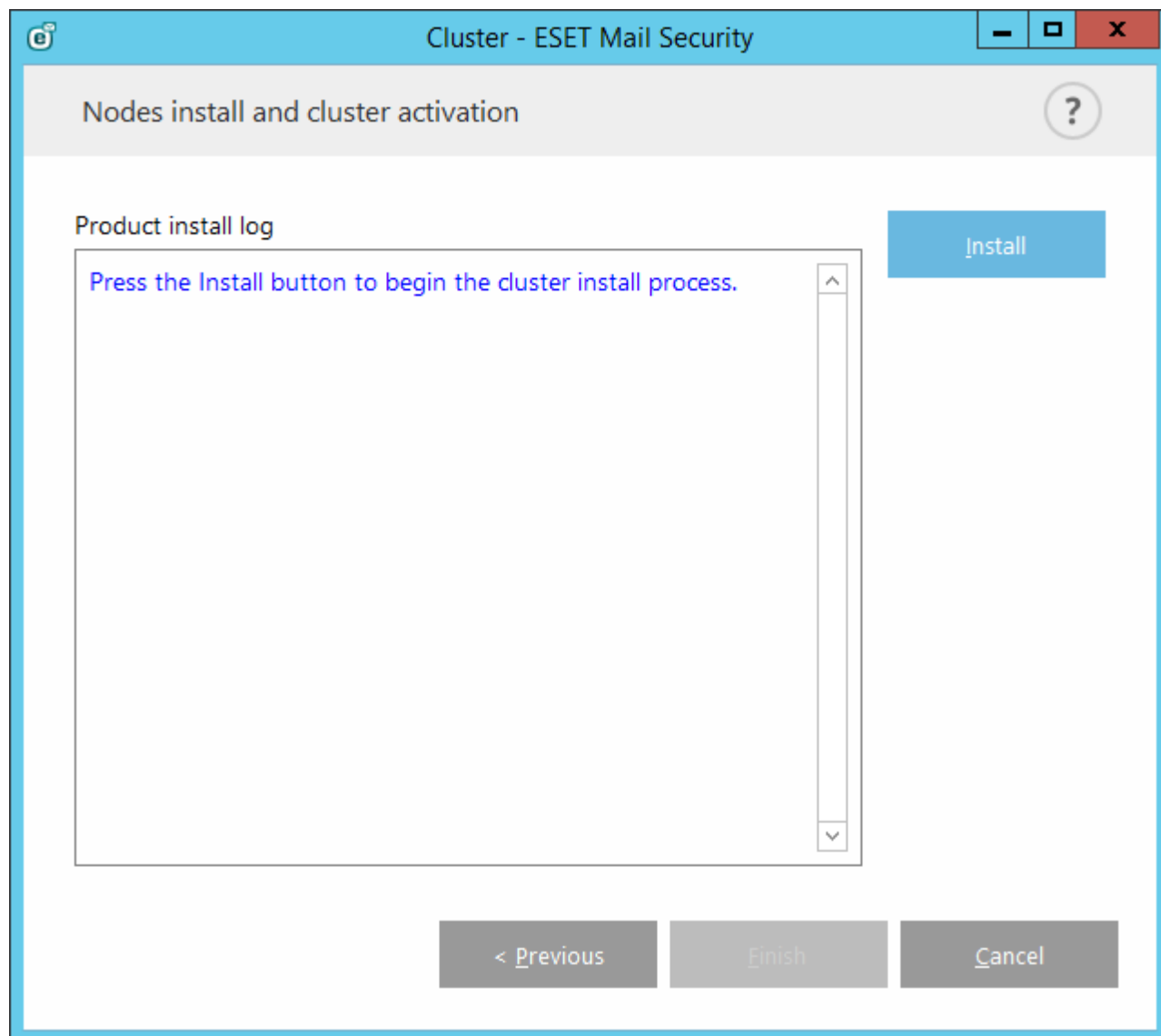
NOTA: se si desidera creare ESET Cluster con architetture di sistemi operativi miste (a 32 e a 64 bit), sarà

necessario installare ESET Mail Security manualmente. Tale condizione verrà rilevata nei passaggi successivi e le informazioni saranno visualizzate nella finestra del registro.

5.1.10.3 Procedura guidata cluster: pagina 3

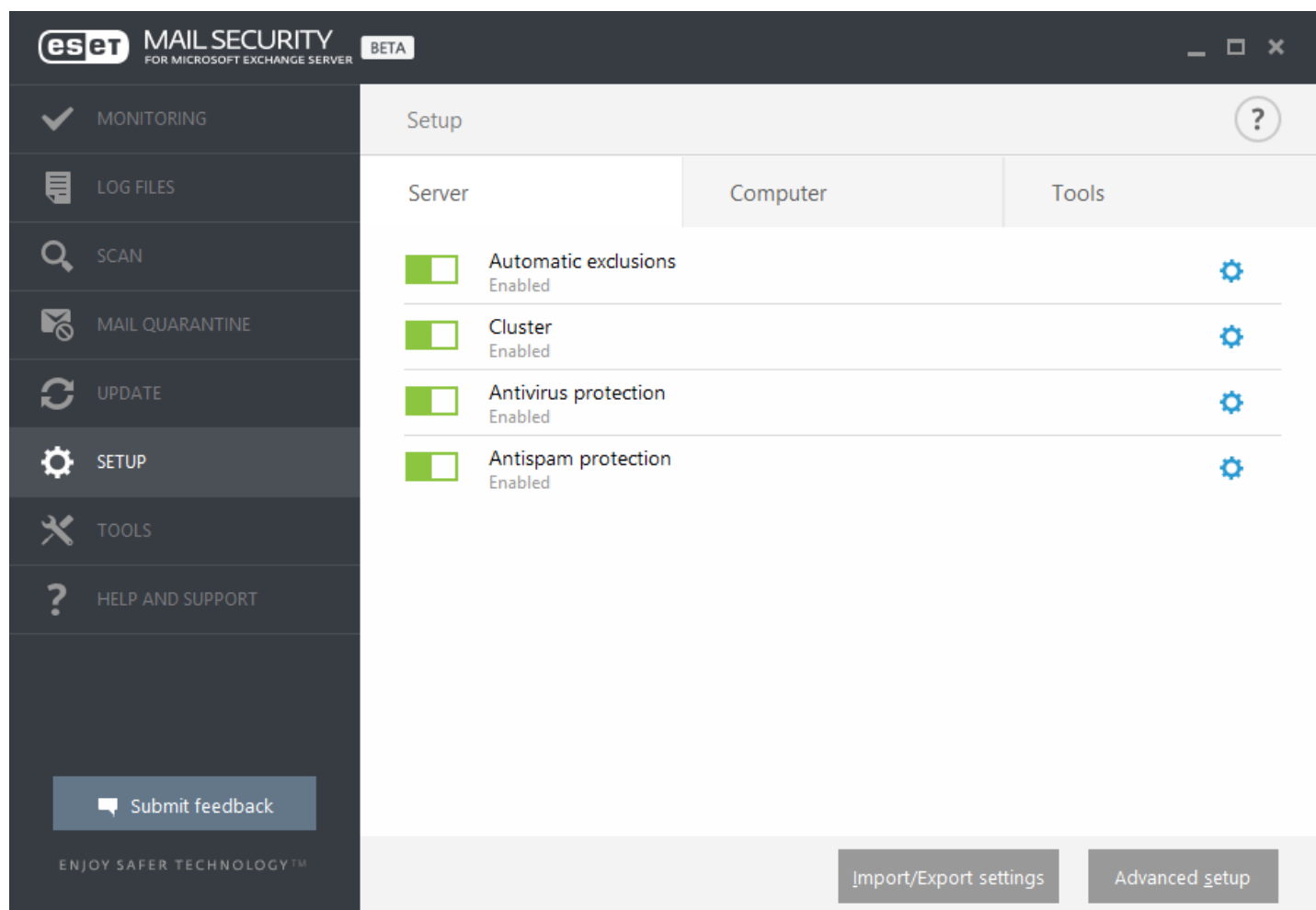
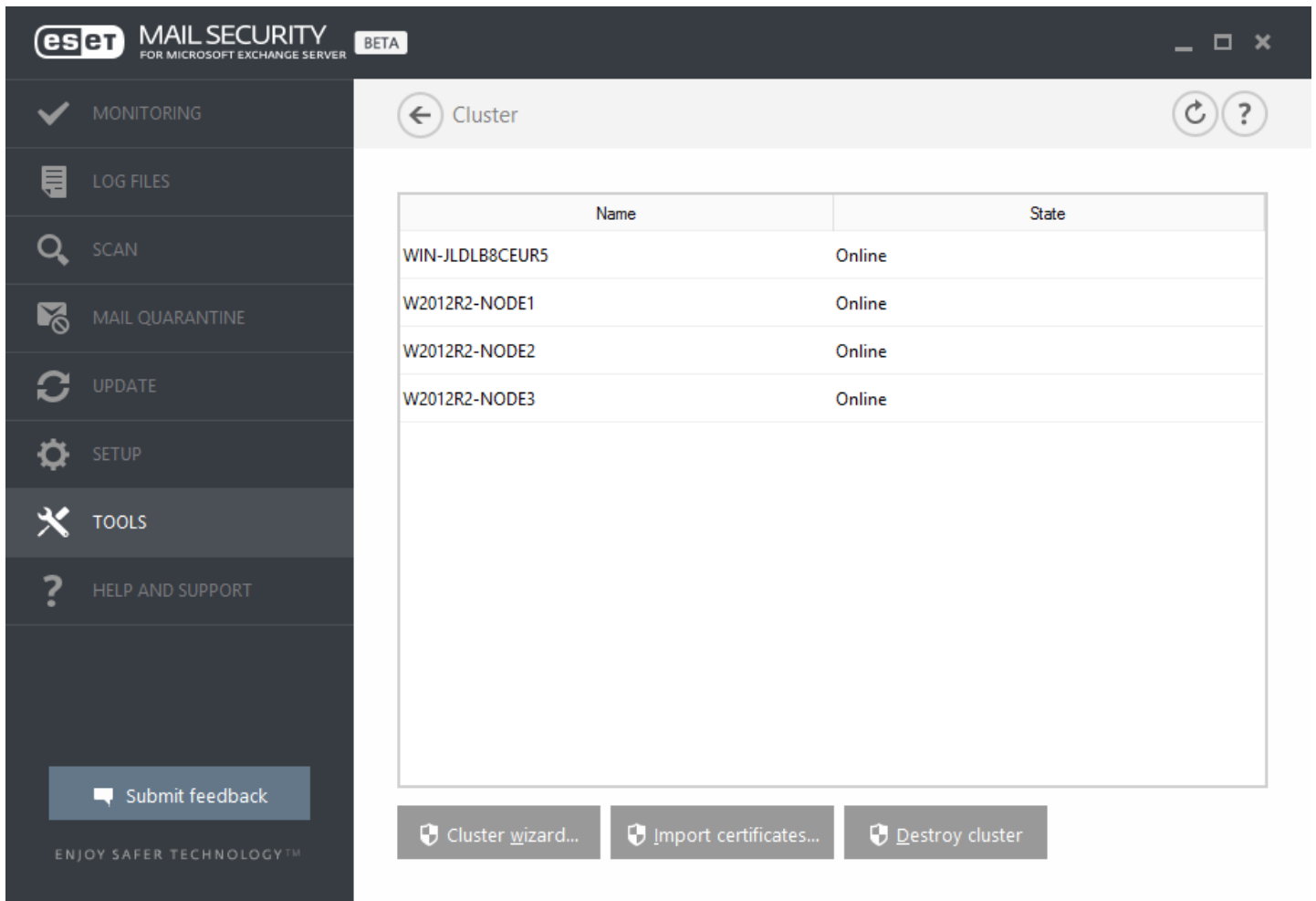
Dopo aver specificato i dettagli di installazione, viene eseguito un controllo del nodo. Nel **Rapporto controllo nodo** verranno visualizzati i seguenti controlli:

- tutti i nodi esistenti sono on-line
- i nuovi nodi sono accessibili
- il nodo è on-line
- la condivisione admin è accessibile
- l'esecuzione remota è possibile
- è installata la versione corretta del prodotto o nessun prodotto (solo se è installata l'opzione installazione automatica)
- sono presenti i nuovi certificati

Al termine del controllo del nodo, verrà visualizzato il rapporto:

5.1.10.4 Procedura guidata cluster: pagina 4

In caso di installazione del prodotto su una macchina remota durante l'inizializzazione di ESET Cluster, il pacchetto del programma di installazione viene ricercato nella directory %ProgramData%\ESET\<Produt_name>\Installer. Se il pacchetto di installazione non viene trovato in tale percorso, all'utente viene richiesto di individuarlo.

NOTA: quando si cerca di utilizzare l'installazione remota automatica per un nodo con una piattaforma differente (a 32 bit invece che a 64 bit), questo verrà rilevato e ne verrà consigliata l'installazione manuale.

NOTA: se si è in possesso di una versione precedente di ESET Mail Security già installata su alcuni nodi, sarà necessario reinstallare una versione più recente di ESET Mail Security su queste macchine prima della creazione del cluster. Tale operazione potrebbe causare un riavvio automatico delle macchine. In questi casi, l'utente visualizzerà un avviso.

Cluster - ESET Mail Security
Nodes install and cluster activation
Product install log
Install
[4:53:08 PM] Generating certificates for cluster nodes...
[4:53:11 PM] All certificates created.
[4:53:11 PM] Copying files to remote machines:
[4:53:12 PM] All files have been copied to remote machines.
[4:53:12 PM] Installing product:
[4:53:36 PM] ESET solutions are installed on all remote machines.
[4:53:37 PM] Enrolling certificates:
[4:53:42 PM] All certificates have been enrolled to remote machines.
[4:53:42 PM] Activating cluster feature:
[4:53:48 PM] Cluster feature has been activated on all machines.
[4:53:48 PM] Pushing license to the nodes:
[4:53:49 PM] License has been successfully pushed to the nodes.
[4:53:49 PM] Synchronizing settings:
[4:53:52 PM] Settings have been synchronized.
< Previous
Finish
Cancel

Dopo averlo configurato correttamente, ESET Cluster verrà visualizzato nella pagina **Configurazione** > **Server** come attivato.

È inoltre possibile controllarne lo stato corrente nella pagina Stato cluster (**Strumenti** > **Cluster**).

Importa certificati...

- Accedere alla cartella contenente i certificati (generati durante l'utilizzo della Procedura guidata cluster).
- Selezionare il file del certificato e fare clic su **Apri**.

5.2 Computer

Il modulo **Computer** , disponibile in **Configurazione** > **Computer**, consente di visualizzare una panoramica dei moduli di protezione descritti nel capitolo precedente. In questa sezione, sono disponibili le seguenti impostazioni:

- Protezione file system in tempo reale
- Controllo del computer su richiesta
- Controllo stato di inattività
- Controllo all'avvio
- Supporti rimovibili
- Protezione documenti
- HIPS

Le **Opzioni di controllo** per tutti i moduli di protezione (ad esempio, protezione file system in tempo reale, protezione accesso Web, ecc.) consentono all'utente di attivare o disattivare il rilevamento dei seguenti elementi:

- Le applicazioni potenzialmente indesiderate (PUA) non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso.
  Per ulteriori informazioni su questi tipi di applicazioni, consultare la relativa voce del glossario.
- Le applicazioni potenzialmente pericolose sono software commerciali legittimi che potrebbero essere utilizzati in modo non conforme per scopi illegittimi. Esempi di applicazioni potenzialmente pericolose sono strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano ciascuna battuta digitata da un utente). Questa opzione è disattivata per impostazione predefinita.

Per ulteriori informazioni su questi tipi di applicazioni, consultare la relativa voce del glossario.

- Le **Applicazioni potenzialmente sospette** includono programmi compressi mediante programmi di compressione o protettori. Questi tipi di programmi di protezione sono spesso utilizzati dagli autori di malware per eludere il rilevamento.

La **Tecnologia Anti-Stealth** è un sistema sofisticato in grado di rilevare programmi pericolosi, come ad esempio i rootkit, che sono in grado di nascondersi dal sistema operativo. Ciò significa che non è possibile rilevarli mediante l'utilizzo di tecniche di testing ordinarie.

La funzione esclusioni processi consente all'utente di escludere processi specifici. Ad esempio, nel caso dei processi della soluzione di backup, tutte le operazioni dei file attribuite a questi processi esclusi vengono ignorate e considerate sicure, riducendo in tal modo l'interferenza con il processo di backup.

Le esclusioni consentono all'utente di escludere file e cartelle dal controllo. Per garantire che la ricerca delle minacce venga eseguita su tutti gli oggetti, si consiglia di creare esclusioni solo se assolutamente necessario. Le situazioni in cui potrebbe essere necessario escludere un oggetto potrebbero includere, ad esempio, il controllo di voci di database di grandi dimensioni che rallenterebbero il computer durante un controllo o di un software che entra in conflitto con il controllo. Per consultare le istruzioni relative all'esclusione di un oggetto dal controllo, consultare Esclusioni.

5.2.1 Rilevamento di un'infiltrazione

Le infiltrazioni possono raggiungere il sistema da diversi accessi, ad esempio pagine Web, cartelle condivise, messaggi e-mail o dispositivi rimovibili (USB, dischi esterni, CD, DVD, dischi e così via).

Comportamento standard

In linea generale, ESET Mail Security gestisce le infiltrazioni utilizzando i seguenti strumenti per la rilevazione:

- Protezione file system in tempo reale
- Protezione accesso Web
- Protezione client di posta
- Controllo del computer su richiesta

Ciascuna di tali opzioni utilizza il livello di pulizia standard e tenta di pulire il file e di spostarlo nella Quarantena o di interrompere la connessione. Una finestra di avviso viene visualizzata nell'area di notifica posta nell'angolo in basso a destra della schermata. Per ulteriori informazioni sui livelli di pulizia e sul comportamento, vedere Pulizia.

Pulizia ed eliminazione

In assenza di azioni predefinite per l'esecuzione della Protezione file system in tempo reale, verrà chiesto all'utente di selezionare un'opzione nella finestra di avviso. Le opzioni generalmente disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione**, in quanto i file infettati non verranno puliti. È opportuno selezionare questa opzione solo quando si è certi che un file non è pericoloso e che si tratta di un errore di rilevamento.

Applicare la pulizia nel caso in cui un file sia stato attaccato da un virus che ha aggiunto un codice dannoso. In tal caso, tentare innanzitutto di pulire il file infetto per ripristinarne lo stato originale. Nel caso in cui il file sia composto esclusivamente da codice dannoso, verrà eliminato.

Se un file infetto è "bloccato" o utilizzato da un processo del sistema, verrà eliminato solo dopo essere stato rilasciato (generalmente dopo il riavvio del sistema).

Minacce multiple

Se durante un controllo del computer i file infetti non sono stati puliti (o se il Livello di pulizia era impostato su **Nessuna pulizia**), viene visualizzata una finestra di avviso che richiede di selezionare un'azione per i file in questione. Selezionare le azioni da eseguire sui file (le azioni vengono impostate singolarmente per ciascun file presente nell'elenco), quindi fare clic su **Fine**.

Eliminazione dei file negli archivi

In modalità di pulizia predefinita, l'intero archivio verrà eliminato solo nel caso in cui contenga file infetti e nessun file pulito. In pratica, gli archivi non vengono eliminati nel caso in cui dovessero contenere anche file puliti non dannosi. Durante l'esecuzione di un controllo di massima pulizia, si consiglia di agire con estrema prudenza, in quanto, in caso di rilevamento di un file infetto, verrà eliminato l'intero archivio di appartenenza dell'oggetto, indipendentemente dallo stato degli altri file.
Se il computer mostra segnali di infezione malware, ad esempio appare più lento, si blocca spesso e così via, è consigliabile attenersi alle seguenti istruzioni:

- Aprire ESET Mail Security e fare clic su Controllo del computer
- Fare clic su **Controllo intelligente** (per ulteriori informazioni, consultare Controllo del computer)
- Al termine del controllo, consultare il rapporto per conoscere il numero di file controllati, infetti e puliti

Se si desidera controllare solo una parte del disco, fare clic su **Controllo personalizzato** e selezionare le destinazioni su cui effettuare un controllo antivirus.

5.2.2 Esclusioni processi

Questa funzione consente all'utente di escludere i processi delle applicazioni dal controllo antivirus all'accesso. Queste esclusioni aiutano a ridurre al minimo il rischio di potenziali conflitti e a migliorare le prestazioni delle applicazioni escluse. Tale condizione registra, a sua volta, un effetto positivo sulle prestazioni generali del sistema operativo.

L'esclusione di un processo determina il mancato monitoraggio del relativo file eseguibile. L'attività del processo escluso non è monitorata da ESET Mail Security e non viene eseguito alcun controllo sulle operazioni dei file effettuate dal processo.

Utilizzare **Aggiungi**, **Modifica** e **Rimuovi** per gestire le esclusioni dei processi.

NOTA: le esclusioni dei processi sono esclusioni riguardanti esclusivamente il controllo antivirus all'accesso. Ad esempio, la protezione accesso Web non tiene conto di questa esclusione. Di conseguenza, in caso di esclusione del file eseguibile del browser Web in uso, il controllo dei file scaricati continua a essere eseguito. In tal modo, risulta ancora possibile rilevare un'infiltrazione. Poiché lo scenario illustrato è solo un esempio, si sconsiglia di creare esclusioni per i browser Web.

NOTA: l'HIPS viene utilizzato ai fini della valutazione dei processi esclusi. Si consiglia pertanto di testare i nuovi processi esclusi attivando l'HIPS (o disattivandolo in caso di problemi). La disattivazione dell'HIPS non inciderà sulle esclusioni dei processi. In caso di disattivazione dell'HIPS, l'identificazione dei processi esclusi si baserà esclusivamente sul percorso.

5.2.3 Esclusioni automatiche

Gli sviluppatori delle applicazioni server e dei sistemi operativi consigliano di escludere i gruppi di file e cartelle di lavoro critici dai controlli antivirus per la maggior parte dei loro prodotti. I controlli antivirus possono esercitare un'influenza negativa sulle prestazioni di un server, creando conflitti e impedendo persino l'esecuzione di alcune applicazioni sul server. Le esclusioni aiutano a ridurre al minimo il rischio di potenziali conflitti e a migliorare le prestazioni generali del server quando è in esecuzione il software antivirus.

ESET Mail Security identifica le applicazioni server e i file del sistema operativo del server critici e li aggiunge automaticamente all'elenco di Esclusioni. È possibile visualizzare un elenco di applicazioni server rilevate sotto a **Esclusioni automatiche da generare** per le quali sono state create le esclusioni. Tutte le esclusioni automatiche sono attivate per impostazione predefinita. È possibile disattivare/attivare ciascuna applicazione server facendo clic sul pulsante appropriato. Tale operazione genererà il seguente risultato:

1. Se l'esclusione di un'applicazione/un sistema operativo rimane attivata, uno qualsiasi dei file e delle cartelle critici verrà aggiunto all'elenco di file esclusi dal controllo (**Configurazione avanzata** > > **Di base** > **Esclusioni** > **Modifica**). A ogni riavvio del server, il sistema esegue un controllo automatico delle esclusioni e ripristina eventuali esclusioni che potrebbero essere state eliminate dall'elenco. Questa è l'impostazione consigliata se si desidera essere certi che siano sempre applicate le Esclusioni automatiche consigliate.

2. Se l'utente disattiva l'esclusione di un'applicazione/un sistema operativo, i rispettivi file e cartelle critici rimangono nell'elenco di file esclusi dal controllo (**Configurazione avanzata** > > **Di base** > **Esclusioni** > **Modifica**). Tuttavia, non verranno controllati e rinnovati automaticamente sull'elenco **Esclusioni** a ogni riavvio del server (vedere precedente punto 1). Questa impostazione è consigliata agli utenti avanzati che desiderano rimuovere o modificare alcune delle esclusioni standard. Se si desidera rimuovere le esclusioni dall'elenco senza riavviare il server, sarà necessario eseguire manualmente l'operazione (**Configurazione avanzata** > > **Di base** > **Esclusioni** > **Modifica**).

Qualsiasi esclusione definita dall'utente e inserita manualmente (in **Configurazione avanzata** > > **Di base** > **Esclusioni** > **Modifica**) non sarà influenzata dalle impostazioni descritte in precedenza.

Le Esclusioni automatiche di applicazioni/sistemi operativi server vengono selezionate in base alle raccomandazioni Microsoft. Per ulteriori informazioni, consultare i seguenti articoli della Knowledge Base Microsoft:

- Consigli sul controllo antivirus per i computer Enterprise sui quali vengono eseguite versioni attualmente supportate di Windows
- Consigli per la risoluzione di problemi relativi a un computer Exchange Server su cui è installato un software antivirus
- Controllo antivirus dei file su Exchange 2007
- Software antivirus nel sistema operativo sui server Exchange

5.2.4 Cache locale condivisa

La cache locale condivisa potenzierà le prestazioni negli ambienti virtuali eliminando i controlli duplicati nella rete. Ciò garantisce un controllo unico di ciascun file e l'archiviazione nella cache condivisa. Attivare il pulsante **Opzione memorizzazione nella cache** per salvare le informazioni relative ai controlli di file e cartelle presenti nella rete dell'utente nella cache locale. Se si esegue un nuovo controllo, ESET Mail Security ricercherà i file controllati nella cache. In caso di corrispondenza tra i file, questi verranno esclusi dal controllo.

La **Configurazione** del server cache contiene i seguenti elementi**:**

- **Nome host**: nome o indirizzo IP del computer in cui è collocata la cache.
- **Porta**: numero della porta utilizzata per la comunicazione (identico a quello impostato nella cache locale condivisa).
- **Password**: specificare la password della cache locale se necessario.

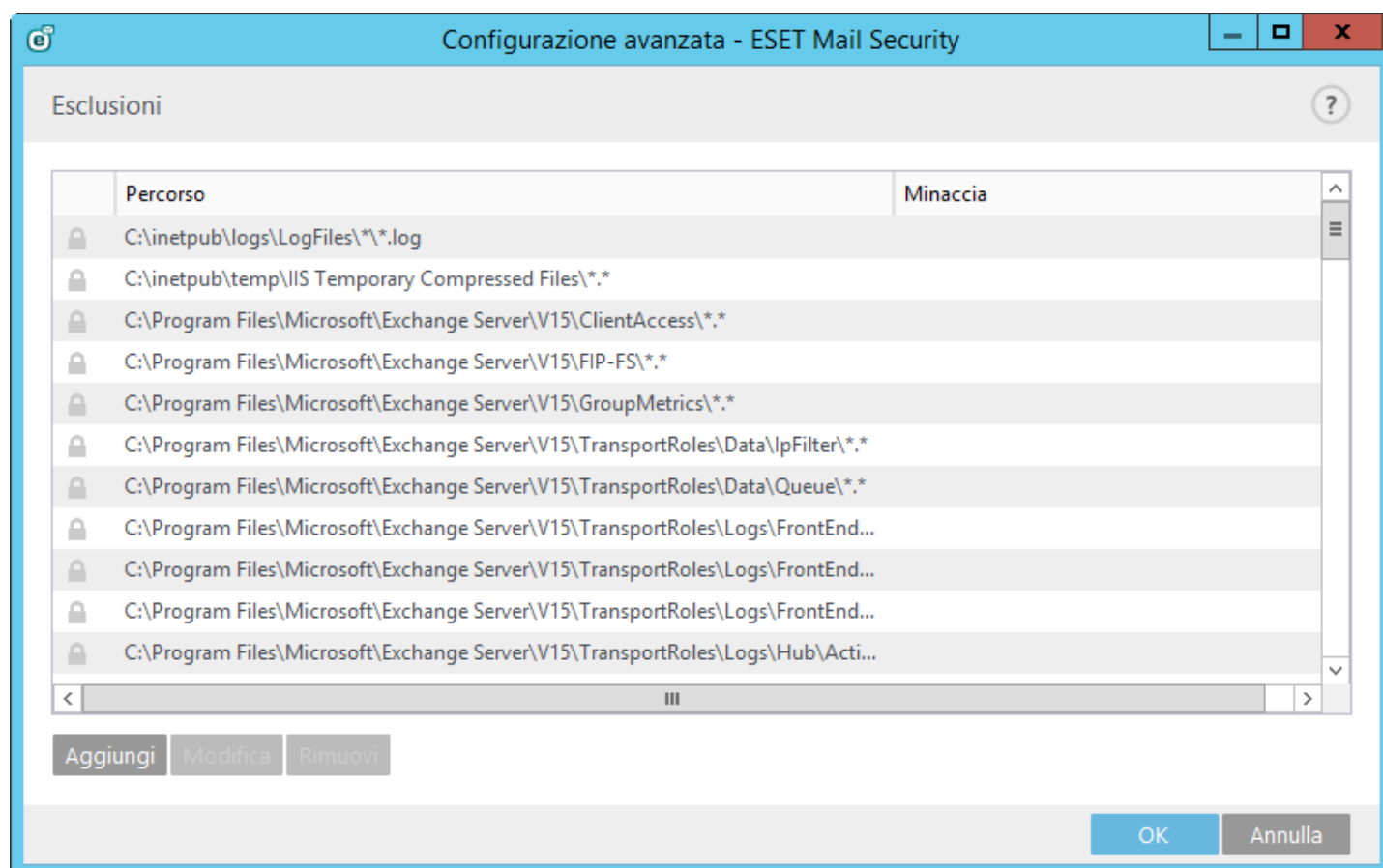
5.2.5 Prestazioni

È possibile impostare un numero di motori di controllo ThreatSense indipendenti utilizzati dalla protezione antivirus e antispyware in un momento specifico.

In assenza di altre restrizioni, si consiglia di aumentare il numero di motori di controllo ThreatSense in base a questa formula: *numero di motori di controllo ThreatSense = (numero di CPU fisiche x 2) + 1*.

NOTA: il valore accettabile è compreso tra 1 e 20. È possibile pertanto utilizzare un numero massimo di 20 motori di controllo ThreatSense.

5.2.6 Protezione file system in tempo reale

La funzione di Protezione file system in tempo reale consente di controllare tutti gli eventi correlati all'antivirus nel sistema. Su tutti i file vengono ricercati codici dannosi al momento dell'apertura, creazione o esecuzione sul computer. La funzione Protezione file system in tempo reale viene avviata all'avvio del sistema.

Per impostazione predefinita, la protezione file system in tempo reale viene avviata all'avvio del sistema e fornisce un controllo ininterrotto. In casi particolari (ad esempio, in caso di conflitto con un altro scanner in tempo reale), la protezione in tempo reale può essere disattivata deselezionando **Avvia automaticamente la protezione file system in tempo reale** in Configurazione avanzata sotto a **Protezione file system in tempo reale**> **Standard**.

- **Supporti da controllare**

Per impostazione predefinita, vengono controllati tutti i tipi di supporto alla ricerca di eventuali minacce:

Dischi locali: controlla tutti gli hard disk del sistema.
Supporti rimovibili: controlla CD/DVD, supporti di archiviazione USB, dispositivi Bluetooth e così via.
Dischi di rete: esegue il controllo di tutte le unità mappate.

Si consiglia di utilizzare le impostazioni predefinite e di modificarle solo in casi specifici, ad esempio quando il controllo di alcuni supporti rallenta notevolmente il trasferimento dei dati.

- **Controlla**

Per impostazione predefinita, tutti i file vengono controllati al momento dell'apertura, creazione o esecuzione. Si consiglia di mantenere le seguenti impostazioni predefinite per garantire il massimo livello di protezione in tempo reale per il computer in uso:

- **Apertura dei file**: attiva o disattiva il controllo al momento dell'apertura dei file.
- **Creazione dei file**: attiva o disattiva il controllo al momento della creazione dei file.
- **Esecuzione dei file**: attiva o disattiva il controllo al momento dell'esecuzione dei file.
- **Accesso supporti rimovibili**: attiva o disattiva il controllo attivato dall'accesso a determinati supporti rimovibili dotati di uno spazio di archiviazione.
- **Arresto computer**: attiva o disattiva il controllo attivato dall'arresto del computer.

La Protezione file system in tempo reale, che viene attivata da vari eventi di sistema, tra cui l'accesso a un file, controlla tutti i tipi di supporti. Grazie ai metodi di rilevamento della tecnologia ThreatSense (descritti nella sezione Parametri ThreatSense), è possibile configurare la Protezione file system in tempo reale allo scopo di gestire i file di nuova creazione in base a modalità diverse rispetto a quelle utilizzate per i file esistenti. Ad esempio, la Protezione file system in tempo reale può essere configurata in modo da monitorare più da vicino i file di nuova creazione.

Per ridurre al minimo l'impatto sul sistema della protezione in tempo reale, i file che sono già stati controllati verranno ignorati, eccetto nel caso in cui siano state apportate modifiche. I file vengono controllati nuovamente subito dopo ogni aggiornamento del database delle firme antivirali. Questo comportamento viene controllato mediante l'utilizzo dell'**Ottimizzazione intelligente**. Se l'ottimizzazione intelligente è disattivata, tutti i file verranno controllati a ogni accesso. Per modificare questa impostazione, premere **F5** per aprire Configurazione avanzata ed espandere **Antivirus** > **Protezione file system in tempo reale**. Fare clic su **Parametri ThreatSense** > **Altro** e selezionare o deselezionare **Attiva ottimizzazione intelligente**.

5.2.6.1 Esclusioni

Da non confondere con la funzione **Estensioni escluse**

Le esclusioni consentono all'utente di escludere file e cartelle dal controllo. Per garantire che la ricerca delle minacce venga eseguita su tutti gli oggetti, si consiglia di creare esclusioni solo se assolutamente necessario. Le situazioni in cui potrebbe essere necessario escludere un oggetto includono, ad esempio, il controllo di voci di database di grandi dimensioni che rallenterebbero il computer durante un controllo o di un software che entra in conflitto con il controllo (ad esempio, software di backup).

Per escludere un oggetto dal controllo:

Fare clic su **Aggiungi** e inserire il percorso a un oggetto oppure selezionarlo nella struttura ad albero.
È possibile utilizzare i caratteri jolly per includere un gruppo di file. Un punto interrogativo (?) rappresenta un carattere variabile singolo, mentre un asterisco (*) rappresenta una stringa variabile di zero o più caratteri.

Esempi

- Se si desidera escludere tutti i file presenti in una cartella, digitare il percorso della cartella e utilizzare la maschera "*.*".
- Per escludere un'unità intera, compresi tutti i file e le sottocartelle, utilizzare la maschera "D:*".
- Se si desidera escludere solo i file DOC, utilizzare la maschera "*.doc".
- Se il nome di un file eseguibile contiene un determinato numero di caratteri (e i caratteri variano) e si è sicuri solo della prima lettera (ad esempio "D"), utilizzare il formato seguente: "D????.exe". I punti interrogativi sostituiscono i caratteri mancanti (sconosciuti).

i **NOTA:** una minaccia all'interno di un file non sarà rilevata dal modulo di protezione file system in tempo reale o dal modulo del controllo del computer se quel file soddisfa i criteri di esclusione dal controllo.

Colonne

Percorso: percorso dei file e delle cartelle esclusi.
Minaccia: se viene visualizzato il nome di una minaccia accanto a un file escluso, ciò significa che il file viene escluso

soltanto per quella specifica minaccia. Se il file si infetta successivamente con altri malware, verrà rilevato dal modulo antivirus. Questo tipo di esclusione, che può essere utilizzato esclusivamente per alcuni tipi di infiltrazioni, può essere creato nella finestra di avviso delle minacce che segnala l'infiltrazione (fare clic su **Mostra opzioni avanzate**, quindi selezionare **Escludi dal rilevamento**) oppure facendo clic su **Configurazione** > **Quarantena**, facendo clic con il pulsante destro del mouse sul file in quarantena e selezionando **Ripristina ed escludi dal rilevamento** dal menu contestuale.

Elementi di controllo

Aggiungi: esclude gli oggetti dal rilevamento.
Modifica: consente all'utente di modificare le voci selezionate.
Rimuovi: rimuove le voci selezionate.

5.2.6.1.1 Aggiungi o modifica esclusione

Questa finestra di dialogo consente di aggiungere o modificare le esclusioni. L'operazione può essere eseguita in due modi:

- digitando il percorso di un oggetto da escludere oppure
- selezionando l'oggetto nella struttura ad albero (fare clic su **...** alla fine del campo di testo da ricercare)

Se si utilizza il primo metodo, è possibile utilizzare i caratteri jolly descritti nella sezione Formato di esclusione.

5.2.6.1.2 Formato di esclusione

È possibile utilizzare i caratteri jolly per includere un gruppo di file. Un punto interrogativo (?) rappresenta un carattere variabile singolo, mentre un asterisco (*) rappresenta una stringa variabile di zero o più caratteri.

Esempi

- Se si desidera escludere tutti i file presenti in una cartella, digitare il percorso della cartella e utilizzare la maschera "*.*".
- Per escludere un'unità intera, compresi tutti i file e le sottocartelle, utilizzare la maschera "D:*".
- Se si desidera escludere solo i file DOC, utilizzare la maschera "*.doc".
- Se il nome di un file eseguibile contiene un determinato numero di caratteri (e i caratteri variano) e si è sicuri solo della prima lettera (ad esempio "D"), utilizzare il formato seguente: "D????.exe". I punti interrogativi sostituiscono i caratteri mancanti (sconosciuti).

5.2.6.2 Parametri di ThreatSense

ThreatSense è una tecnologia che prevede numerosi metodi di rilevamento di minacce complesse. Questa tecnologia è proattiva, ovvero fornisce protezione anche durante le prime ore di diffusione di una nuova minaccia. Il programma utilizza una combinazione di analisi del codice, emulazione del codice, firme generiche e firme antivirali che operano in modo integrato per potenziare enormemente la protezione del sistema. Il motore di controllo è in grado di controllare contemporaneamente diversi flussi di dati, ottimizzando l'efficienza e la percentuale di rilevamento. La tecnologia ThreatSense è inoltre in grado di eliminare i rootkit.

Le opzioni di configurazione del motore ThreatSense consentono all'utente di specificare vari parametri di controllo:

- Tipi ed estensioni dei file da controllare
- Combinazione di diversi metodi di rilevamento
- Livelli di pulizia e così via.

Per accedere alla finestra di configurazione, fare clic su **Configurazione parametri motore ThreatSense** nella finestra Configurazione avanzata di qualsiasi modulo che utilizza la tecnologia ThreatSense (vedere sezione sottostante). Scenari di protezione diversi potrebbero richiedere configurazioni diverse. Partendo da questo presupposto, ThreatSense è configurabile singolarmente per i seguenti moduli di protezione:

- Protezione file system in tempo reale
- Controllo stato di inattività
- Controllo all'avvio
- Protezione documenti
- Protezione client di posta
- Protezione accesso Web
- Controllo computer

I parametri di ThreatSense vengono ottimizzati per ciascun modulo e la relativa modifica può influire in modo significativo sul funzionamento del sistema. Ad esempio, la modifica dei parametri per il controllo degli eseguibili compressi o per consentire l'euristica avanzata nel modulo della protezione file system in tempo reale potrebbe causare un rallentamento del sistema (questi metodi di controllo vengono applicati generalmente solo ai file di nuova creazione). È quindi consigliabile non modificare i parametri predefiniti di ThreatSense per tutti i moduli, ad eccezione di Controllo computer.

Oggetti da controllare

Questa sezione consente all'utente di definire i componenti e i file del computer nei quali verranno ricercate le infiltrazioni.

- **Memoria operativa**: ricerca le minacce che attaccano la memoria operativa del sistema.
- **Settori di avvio**: controlla i settori di avvio alla ricerca di virus nel record di avvio principale.
- **File di e-mail**: il programma supporta le seguenti estensioni: DBX (Outlook Express) ed EML.
- **Archivi**: il programma supporta le seguenti estensioni: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE e molte altri ancora.
- **Archivi autoestraenti**: gli archivi autoestraenti (SFX) sono archivi che non necessitano di programmi speciali, ovvero archivi, per decomprimersi.
- **Eseguibili compressi**: dopo essere stati eseguiti, gli eseguibili compressi (diversamente dai tipi di archivi standard) si decomprimono nella memoria. Oltre agli eseguibili compressi statici standard (UPS, yoda, ASPack, FSG e così via), lo scanner è in grado di riconoscere numerosi altri tipi di programmi di compressione grazie all'utilizzo dell'emulazione del codice.

Opzioni di controllo

Selezionare i metodi utilizzati durante la ricerca di infiltrazioni nel sistema. Sono disponibili le seguenti opzioni:

- **Euristica**: l'euristica è un algoritmo che analizza l'attività (dannosa) dei programmi. Il vantaggio principale offerto da questa tecnologia consiste nella capacità di identificare software dannosi precedentemente inesistenti o non conosciuti dal database delle firme antivirali precedente. Lo svantaggio è una probabilità (minima) di falsi allarmi.
- **Euristica avanzata/DNA/Firme Smart**: l'euristica avanzata si basa su un algoritmo di euristica esclusivo sviluppato da ESET, ottimizzato per il rilevamento dei worm e dei trojan horse e scritto in linguaggi di programmazione di alto livello. L'utilizzo dell'euristica avanzata determina un aumento esponenziale delle capacità di rilevamento delle minacce dei prodotti ESET. Le firme sono in grado di rilevare e identificare i virus in modo affidabile. Grazie al sistema di aggiornamento automatico, le nuove firme sono disponibili entro poche ore dal rilevamento di una minaccia. Lo svantaggio delle firme consiste nel fatto che tali strumenti rilevano solo i virus conosciuti (o versioni leggermente diverse di questi virus).

Le **Applicazioni potenzialmente indesiderate** (PUA) non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso prima dell'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

- Nuove finestre mai visualizzate in precedenza (popup, annunci pubblicitari)
- Attivazione ed esecuzione di processi nascosti
- Maggiore utilizzo delle risorse del sistema
- Modifiche dei risultati di ricerca
- Applicazione che comunica con server remoti

- **Applicazioni potenzialmente pericolose**: applicazioni potenzialmente pericolose è la classificazione utilizzata per programmi commerciali e legittimi, quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano le battute digitate da un utente). Questa opzione è disattivata per impostazione predefinita.
- **ESET Live Grid**: grazie alla tecnologia di reputazione di ESET, le informazioni sui file controllati vengono verificate rispetto ai dati di ESET Live Grid basato sul cloud, allo scopo di migliorare il rilevamento e la velocità di controllo.

Pulizia

Le impostazioni di pulizia determinano il comportamento dello scanner durante la pulizia di file infetti. Sono disponibili 3 livelli di pulizia:

Nessuna pulizia: i file infetti non vengono puliti automaticamente. Verrà visualizzata una finestra di avviso per consentire all'utente di scegliere un'azione. Questo livello è indicato per utenti più esperti in grado di eseguire le azioni appropriate in caso di infiltrazione.

Pulizia normale: il programma tenterà di pulire o eliminare automaticamente un file infetto in base a un'azione predefinita (a seconda del tipo di infiltrazione). Una notifica nell'angolo in basso a destra della schermata segnalerà il rilevamento e l'eliminazione di un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma offre altre azioni di follow-up. Lo stesso si verifica se non è stato possibile completare un'azione predefinita.

Massima pulizia: il programma pulirà o eliminerà tutti i file infetti. Le uniche eccezioni sono costituite dai file di sistema. Se non è possibile pulire un file, all'utente verrà richiesta l'azione da intraprendere.

Avviso: se un archivio contiene uno o più file infetti, sono disponibili due opzioni per gestire tale archivio. In modalità standard (pulizia standard), l'intero archivio verrà eliminato se tutti i file in esso contenuti sono infetti. In modalità **Massima pulizia**, l'archivio verrà eliminato se contiene almeno un file infetto, indipendentemente dallo stato degli altri file contenuti nell'archivio.

Esclusioni

Un'estensione è la parte del nome di un file delimitata da un punto. Un'estensione definisce il tipo e il contenuto di un file. Questa sezione della configurazione dei parametri di ThreatSense consente di definire i tipi di file da sottoporre a controllo.

Altro

Quando si configurano i parametri del motore ThreatSense per l'esecuzione di un Controllo computer su richiesta, nella sezione **Altro** sono disponibili anche le seguenti opzioni:

- **Flussi di dati alternativi (ADS)**: i flussi di dati alternativi utilizzati dal file system NTFS sono associazioni di file e cartelle invisibili alle normali tecniche di controllo. Molte infiltrazioni tentano di eludere il rilevamento camuffandosi in flussi di dati alternativi.
- **Esegui controlli in background con priorità bassa**: ogni sequenza di controllo utilizza una determinata quantità di risorse del sistema. Se si utilizzano programmi che necessitano di molte risorse di sistema, è possibile attivare il controllo in background con priorità bassa e risparmiare risorse per le applicazioni.
- **Registra tutti gli oggetti**: se questa opzione è selezionata, il file di rapporto riporta tutti i file sottoposti a controllo, anche quelli non infetti. Se ad esempio viene individuata un'infiltrazione all'interno di un archivio, nel rapporto verranno elencati anche i file puliti presenti all'interno dell'archivio.
- **Attiva ottimizzazione intelligente**: al fine di garantire un livello di controllo ottimale, l'attivazione dell'ottimizzazione intelligente consente l'utilizzo delle impostazioni più efficienti mantenendo nel contempo la velocità di controllo più elevata. I vari moduli di protezione eseguono il controllo in modo intelligente, utilizzando metodi di controllo differenti e applicandoli a tipi di file specifici. Se l'opzione di ottimizzazione intelligente non è attiva, durante il controllo verranno applicate solo le impostazioni definite dall'utente nell'architettura ThreatSense dei moduli specifici.
- **Mantieni indicatore data e ora dell'ultimo accesso**: selezionare questa opzione per mantenere l'ora di accesso originale ai file controllati anziché aggiornarli (ad esempio, per l'utilizzo con sistemi di backup di dati).

Limiti

La sezione Limiti consente all'utente di specificare la dimensione massima degli oggetti e i livelli di nidificazione degli archivi sui quali eseguire il controllo:

Impostazioni oggetti

Impostazioni predefinite oggetti

- **Dimensione massima oggetto**: definisce la dimensione massima degli oggetti su cui eseguire il controllo. Il modulo antivirus specifico eseguirà unicamente il controllo degli oggetti di dimensioni inferiori rispetto a quelle specificate. Questa opzione dovrebbe essere modificata solo da utenti esperti che abbiano ragioni particolari per escludere oggetti di maggiori dimensioni dal controllo. Il valore predefinito è: *illimitato*.
- **Durata massima controllo dell'oggetto (sec.)**: definisce il valore temporale massimo per il controllo di un oggetto. Se è stato immesso un valore definito dall'utente, il modulo antivirus interromperà il controllo dell'oggetto una volta raggiunto tale valore, indipendentemente dal fatto che il controllo sia stato completato. Il valore predefinito è: *illimitato*.

Configurazione controllo degli archivi

Livello di nidificazione degli archivi: specifica il livello massimo di controllo degli archivi. Il valore predefinito è: *10*.

Dimensione massima file in archivio: questa opzione consente all'utente di specificare le dimensioni massime dei file contenuti all'interno degli archivi, i quali, una volta estratti, saranno sottoposti a controllo. Il valore predefinito è: *illimitato*.

NOTA: si consiglia di non modificare i valori predefiniti. In circostanze normali, non vi sono motivi particolari per eseguire tale operazione.

5.2.6.2.1 Estensioni escluse

Un'estensione è la parte del nome di un file delimitata da un punto. Un'estensione definisce il tipo e il contenuto di un file. Questa sezione della configurazione dei parametri di ThreatSense consente di definire i tipi di file da sottoporre a controllo.

Per impostazione predefinita, vengono controllati tutti i file. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dal controllo.

L'esclusione di file è un'operazione utile nel caso in cui il controllo di determinati tipi di file impedisca il corretto funzionamento di uno specifico programma che utilizza determinate estensioni. Ad esempio, potrebbe essere consigliabile escludere le estensioni EDB, EML e TMP durante l'utilizzo dei server Microsoft Exchange.

I pulsanti **Aggiungi** e **Rimuovi** consentono all'utente di attivare o impedire il controllo di estensioni di file specifiche. Per aggiungere una nuova estensione all'elenco, fare clic su Aggiungi tipo di estensione nel campo vuoto e fare clic su OK. Dopo aver selezionato **Inserisci valori multipli**, è possibile aggiungere estensioni di file multiple delimitate da righe, virgole o punti e virgola. Attivando selezioni multiple, sarà possibile visualizzare le estensioni nell'elenco. Per eliminare un'estensione dall'elenco, selezionarla e fare clic su **Rimuovi**. Se si desidera modificare un'estensione selezionata, fare clic su **Modifica**.

I simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco rappresenta qualsiasi stringa di caratteri, mentre il punto interrogativo rappresenta qualsiasi simbolo.

5.2.6.2.2 Parametri ThreatSense aggiuntivi

Parametri ThreatSense aggiuntivi per i file appena creati e modificati: i file appena creati registrano una maggiore probabilità di essere infettati rispetto a quelli esistenti. Per questo motivo il programma controlla tali file con parametri aggiuntivi. Oltre ai comuni metodi di controllo basati sulle firme, viene utilizzata anche la funzione di euristica avanzata, che è in grado di rilevare le nuove minacce prima del rilascio dell'aggiornamento del database delle firme antivirali. Oltre che sui file appena creati, il controllo viene eseguito sui file autoestraenti (SFX) e sugli eseguibili compressi, ovvero file eseguibili compressi internamente. Per impostazione predefinita, gli archivi vengono analizzati fino al 10° livello di nidificazione e controllati indipendentemente dalla loro dimensione effettiva. Per modificare le impostazioni di controllo dell'archivio, disattivare **Impostazioni predefinite controllo degli archivi**.

Per ulteriori informazioni sugli **Eseguibili compressi**, gli **Archivi autoestraenti** e l'**Euristica avanzata**, consultare Configurazione parametri motore ThreatSense.

Parametri ThreatSense aggiuntivi per i file eseguiti: per impostazione predefinita, durante l'esecuzione dei file, viene utilizzata l'Euristica avanzata. Una volta attivata, si consiglia vivamente di mantenere attivi l'Ottimizzazione intelligente e ESET Live Grid, allo scopo di ridurre l'impatto sulle prestazioni del sistema.

5.2.6.2.3 Livelli di pulizia

La protezione in tempo reale prevede tre livelli di pulizia (per accedere alle impostazioni dei livelli di pulizia, fare clic su **Parametri ThreatSense** nella sezione **Protezione file system in tempo reale**, quindi su **Pulizia**).

Nessuna pulizia: i file infetti non vengono puliti automaticamente. Verrà visualizzata una finestra di avviso per consentire all'utente di scegliere un'azione. Questo livello è indicato per utenti più esperti in grado di eseguire le azioni appropriate in caso di infiltrazione.

Pulizia normale: il programma tenterà di pulire o eliminare automaticamente un file infetto in base a un'azione predefinita (a seconda del tipo di infiltrazione). Una notifica nell'angolo in basso a destra della schermata segnalerà il rilevamento e l'eliminazione di un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma offre altre azioni di follow-up. Lo stesso si verifica se non è stato possibile completare un'azione predefinita.

Massima pulizia: il programma pulirà o eliminerà tutti i file infetti. Le uniche eccezioni sono costituite dai file di sistema. Se non è possibile pulire un file, all'utente verrà richiesta l'azione da intraprendere.

Avviso: se un archivio contiene uno o più file infetti, sono disponibili due opzioni per gestire tale archivio. In

modalità standard (pulizia standard), l'intero archivio verrà eliminato se tutti i file in esso contenuti sono infetti. In modalità **Massima pulizia**, l'archivio verrà eliminato se contiene almeno un file infetto, indipendentemente dallo stato degli altri file contenuti nell'archivio.

5.2.6.2.4 Quando modificare la configurazione della protezione in tempo reale

La protezione file system in tempo reale è il componente più importante per il mantenimento della protezione di un sistema. Prestare la massima attenzione quando si modificano i relativi parametri. È consigliabile modificarli solo in casi specifici.

Dopo aver installato ESET Mail Security, tutte le impostazioni vengono ottimizzate al fine di offrire agli utenti il massimo livello di protezione del sistema. Per ripristinare le impostazioni predefinite, fare clic su accanto a ciascuna scheda nella finestra (**Configurazione avanzata** > > **Protezione file system in tempo reale**).

5.2.6.2.5 Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare un file di test da eicar.com. Questo file di test è un file innocuo e rilevabile da tutti i programmi antivirus. Il file è stato creato da EICAR (European Institute for Computer Antivirus Research) per testare la funzionalità dei programmi antivirus. Può essere scaricato all'indirizzo http://www.eicar.org/download/eicar.com

5.2.6.2.6 Cosa fare se la protezione in tempo reale non funziona

In questo capitolo, verranno illustrati i problemi che potrebbero verificarsi durante l'utilizzo della protezione in tempo reale e le modalità di risoluzione.

La protezione in tempo reale è disattivata

Se la protezione in tempo reale è stata inavvertitamente disattivata da un utente, sarà necessario riattivarla. Per riattivare la protezione in tempo reale, selezionare **Configurazione** nella finestra principale del programma e fare clic su **Protezione file system in tempo reale**.

Se la protezione in tempo reale non viene lanciata all'avvio del sistema, è probabile che l'opzione **Avvia automaticamente la protezione file system in tempo reale** non sia stata selezionata. Per attivare l'opzione, accedere a Configurazione avanzata (**F5**) e fare clic su **Computer** > **Protezione file system in tempo reale** > **Standard** nella sezione **Configurazione avanzata**. Assicurarsi di aver attivato **Avvia automaticamente la protezione file system in tempo reale**.

La protezione in tempo reale non rileva né pulisce le infiltrazioni

Verificare che nel computer non siano installati altri programmi antivirus. Se sono attivati contemporaneamente due scudi di protezione in tempo reale, possono entrare in conflitto. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema prima di installare ESET.

La protezione in tempo reale non viene avviata

Se la protezione in tempo reale non viene lanciata all'avvio del sistema (e l'opzione **Avvia automaticamente la protezione file system in tempo reale** è attivata), ciò potrebbe dipendere da un conflitto con altri programmi. Per ricevere assistenza nella risoluzione del problema, si prega di contattare il Supporto tecnico ESET.

5.2.6.2.7 Invio

È possibile decidere le modalità di invio a ESET dei file e delle informazioni statistiche. Selezionare l'opzione **Tramite Remote Administrator o direttamente a ESET** per inviare i file e le statistiche mediante tutti i mezzi disponibili. Selezionare l'opzione **Tramite Remote Administrator** per inviare i file e le statistiche al server di amministrazione remota, garantendo così il successivo invio ai laboratori delle minacce ESET. Se si seleziona **Direttamente a ESET**, tutti i file sospetti e le informazioni statistiche vengono inviati ai laboratori antivirus ESET direttamente dal programma.

In presenza di file in attesa di invio, il pulsante **Invia ora** sarà attivo. Selezionare questo pulsante per inviare immediatamente i file e le informazioni statistiche.

Selezionare **Attiva registrazione** per creare un rapporto sul quale sono registrati gli invii dei file e delle informazioni statistiche.

5.2.6.2.8 Statistiche

Il Sistema di allarme immediato ThreatSense.Net raccoglierà informazioni anonime sul computer degli utenti in relazione alle nuove minacce rilevate. Queste informazioni possono includere il nome dell'infiltrazione, la data e l'ora del rilevamento, la versione del prodotto di protezione ESET, la versione del sistema operativo in uso e le impostazioni di ubicazione. Solitamente, le statistiche vengono inviate ai server ESET una o due volte al giorno.

Di seguito viene riportato un esempio di pacchetto statistico inviato:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8
```

Condizioni di invio: è possibile decidere quando inviare le informazioni statistiche. Se si sceglie l'opzione **Prima possibile**, le informazioni statistiche verranno inviate non appena vengono create. Questa impostazione è adatta se è disponibile una connessione Internet permanente. Se si seleziona **Durante l'aggiornamento**, tutte le informazioni statistiche verranno inviate nel corso del successivo aggiornamento.

5.2.6.2.9 File sospetti

La scheda **File sospetti** consente di configurare il modo in cui le minacce vengono inviate ai laboratori delle minacce ESET.

Se si rileva un file sospetto, è possibile inviarlo per l'analisi ai laboratori delle minacce. Se viene individuata un'applicazione dannosa, essa verrà aggiunta al successivo aggiornamento delle firme antivirali.

È possibile impostare l'invio automatico dei file, oppure selezionare **Chiedi prima di inviare** se si desidera sapere quali file sono stati inviati per l'analisi e confermarne l'invio.

Se non si desidera inviare alcun file, selezionare l'opzione **Non inviare per l'analisi**. La scelta di non inviare i file per l'analisi non influenza l'invio delle informazioni statistiche configurate nella rispettiva impostazione (consultare la sezione Statistiche).

Condizioni di invio: per impostazione predefinita, è selezionata l'opzione **Prima possibile** per l'invio dei file sospetti ai laboratori antivirus ESET. Questa opzione è consigliata se è disponibile una connessione Internet permanente e i file sospetti possono essere inviati immediatamente. Selezionare l'opzione **Durante l'aggiornamento** per caricare i file sospetti su ThreatSense.Net nel corso del successivo aggiornamento.

Filtro di esclusione: il Filtro di esclusione consente di escludere dall'invio determinati file/cartelle. È ad esempio utile escludere file che potrebbero contenere informazioni riservate, quali documenti o fogli di calcolo. Per impostazione predefinita, vengono esclusi i tipi di file più comuni (.doc, ecc.). Se lo si desidera, è possibile aggiungerli all'elenco di file esclusi.

Contatto e-mail (facoltativo): il **Contatto e-mail [facoltativo]** può essere inviato insieme ai file sospetti e potrebbe essere utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. Tenere presente che non si riceverà alcuna risposta da ESET, a meno che non siano richieste ulteriori informazioni.

5.2.7 Controllo del computer su richiesta

In questa sezione vengono illustrate le opzioni per selezionare i parametri di controllo.

Profilo selezionato: serie specifica di parametri utilizzati dallo scanner su richiesta. Per crearne uno nuovo, fare clic su **Modifica** accanto a **Elenco di profili**.

Se si desidera controllare una destinazione specifica, fare clic su **Modifica** accanto a **Destinazioni di controllo** e scegliere un'opzione dal menu a discesa o selezionare destinazioni specifiche dalla struttura (ad albero) della cartella.

La finestra destinazioni di controllo consente all'utente di definire gli oggetti (memoria, unità, settori, file e cartelle) sui quali verranno ricercate le infiltrazioni. Selezionare gli oggetti dalla struttura ad albero contenente un elenco di tutti i supporti disponibili nel computer. Il menu a discesa **Destinazioni di controllo** consente di selezionare gli oggetti da controllare predefiniti.

- **Attraverso le impostazioni di profilo**: consente di selezionare le destinazioni nel profilo di controllo selezionato.
- **Supporti rimovibili**: consente di selezionare dischi, supporti di archiviazione USB, CD/DVD.
- **Unità locali**: consente di selezionare tutti gli hard disk del sistema.
- **Unità di rete**: consente di selezionare tutte le unità di rete mappate.
- **Cartelle condivise**: consente di selezionare tutte le cartelle condivise sul server locale.
- **Nessuna selezione**: consente di annullare tutte le selezioni.

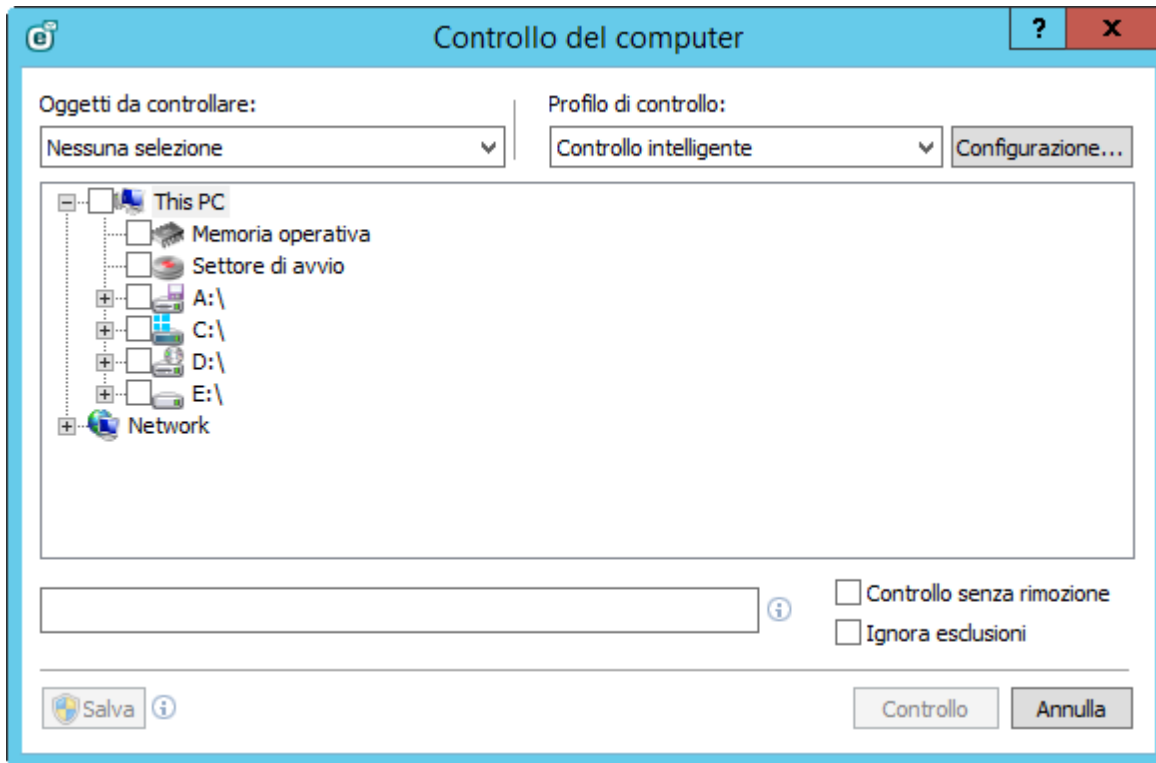
Fare clic su Parametri ThreatSense per modificare i parametri di controllo (ad esempio, metodi di rilevamento) per il controllo del computer su richiesta.

5.2.7.1 Launcher controllo personalizzato

Se si desidera controllare solo una specifica destinazione, è possibile utilizzare lo strumento del controllo personalizzato facendo clic su **Controllo computer** > **Controllo personalizzato** e selezionando un'opzione dal menu a discesa **Destinazioni di controllo** oppure scegliendo destinazioni specifiche dalla struttura (ad albero) della cartella.

La finestra destinazioni di controllo consente all'utente di definire gli oggetti (memoria, unità, settori, file e cartelle) sui quali verranno ricercate le infiltrazioni. Selezionare gli oggetti dalla struttura ad albero contenente un elenco di tutti i supporti disponibili nel computer. Il menu a discesa **Destinazioni di controllo** consente di selezionare gli oggetti da controllare predefiniti.

- **Attraverso le impostazioni di profilo**: consente di selezionare le destinazioni nel profilo di controllo selezionato.
- **Supporti rimovibili**: consente di selezionare dischi, supporti di archiviazione USB, CD/DVD.
- **Unità locali**: consente di selezionare tutti gli hard disk del sistema.
- **Unità di rete**: consente di selezionare tutte le unità di rete mappate.
- **Cartelle condivise**: consente di selezionare tutte le cartelle condivise sul server locale.
- **Nessuna selezione**: consente di annullare tutte le selezioni.

Per visualizzare rapidamente una destinazione di controllo o per aggiungere direttamente una destinazione desiderata (cartella o file), inserirla nel campo vuoto sotto all'elenco delle cartelle. Ciò è possibile solo se nella struttura ad albero non sono state selezionate destinazioni e il menu **Oggetti da controllare** è impostato su **Nessuna selezione**.

Gli elementi infetti non vengono puliti automaticamente. Il controllo senza rimozione può essere utilizzato per ottenere una panoramica dello stato di protezione corrente. Se si desidera effettuare solo un controllo del sistema senza azioni di pulizia aggiuntive, selezionare **Controlla senza pulire**. È inoltre possibile scegliere tra tre livelli di pulizia facendo clic su **Configurazione** > **Parametri ThreatSense** > **Pulizia**. Le informazioni relative al controllo vengono salvate in un rapporto del controllo.

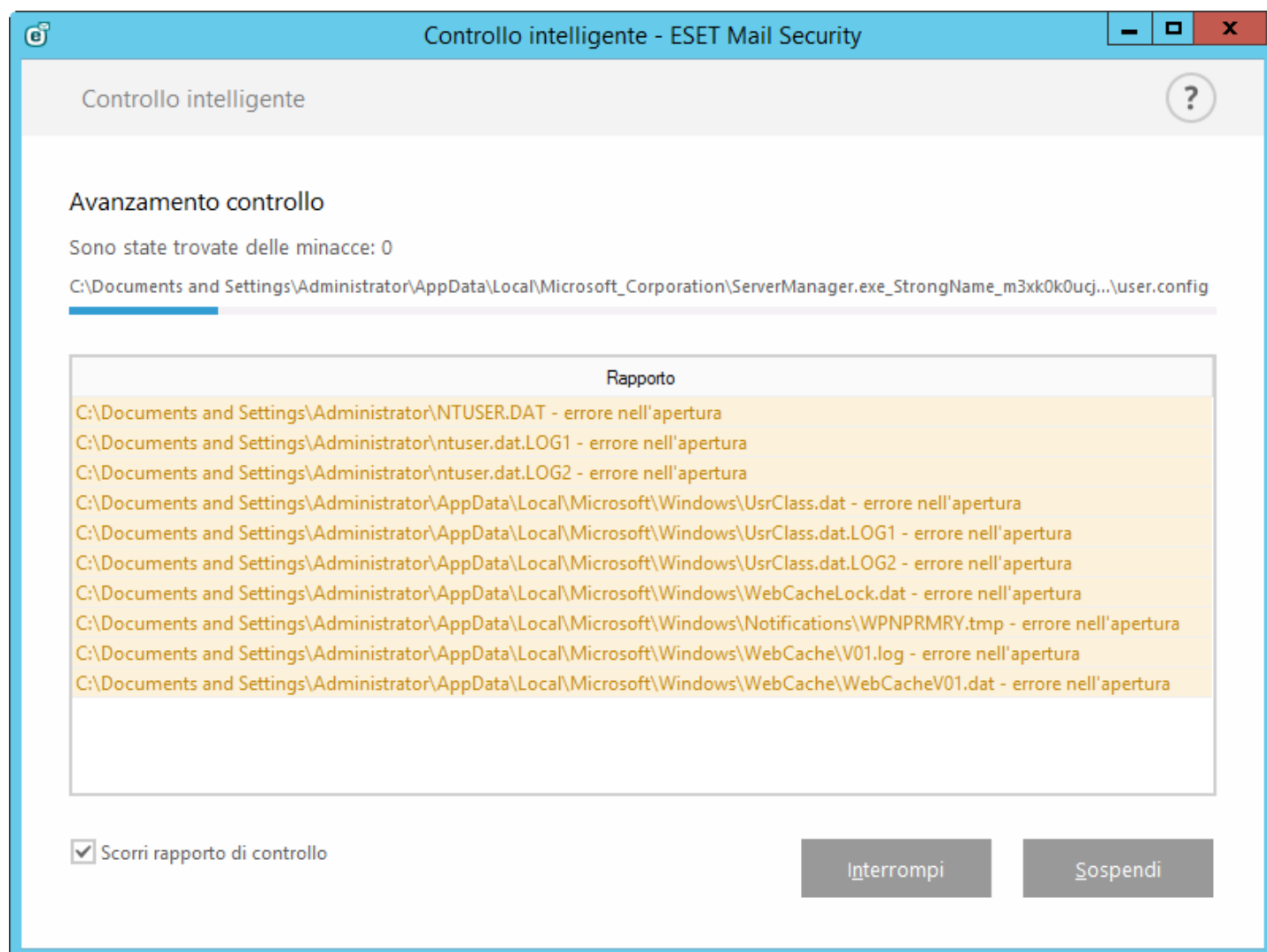
È possibile scegliere un profilo dal menu a discesa **Profilo di controllo** da utilizzare per il controllo delle destinazioni scelte. Il profilo predefinito è **Controllo intelligente**. Esistono due altri profili predefiniti chiamati **Controllo approfondito** e **Controllo menu contestuale**. Questi profili di controllo utilizzano diversi parametri del motore ThreatSense. Fare clic su **Configurazione...** per configurare i dettagli del profilo di controllo scelto nel menu Profilo di controllo. Le opzioni disponibili sono descritte nella sezione **Altro** in Configurazione parametri del motore ThreatSense.

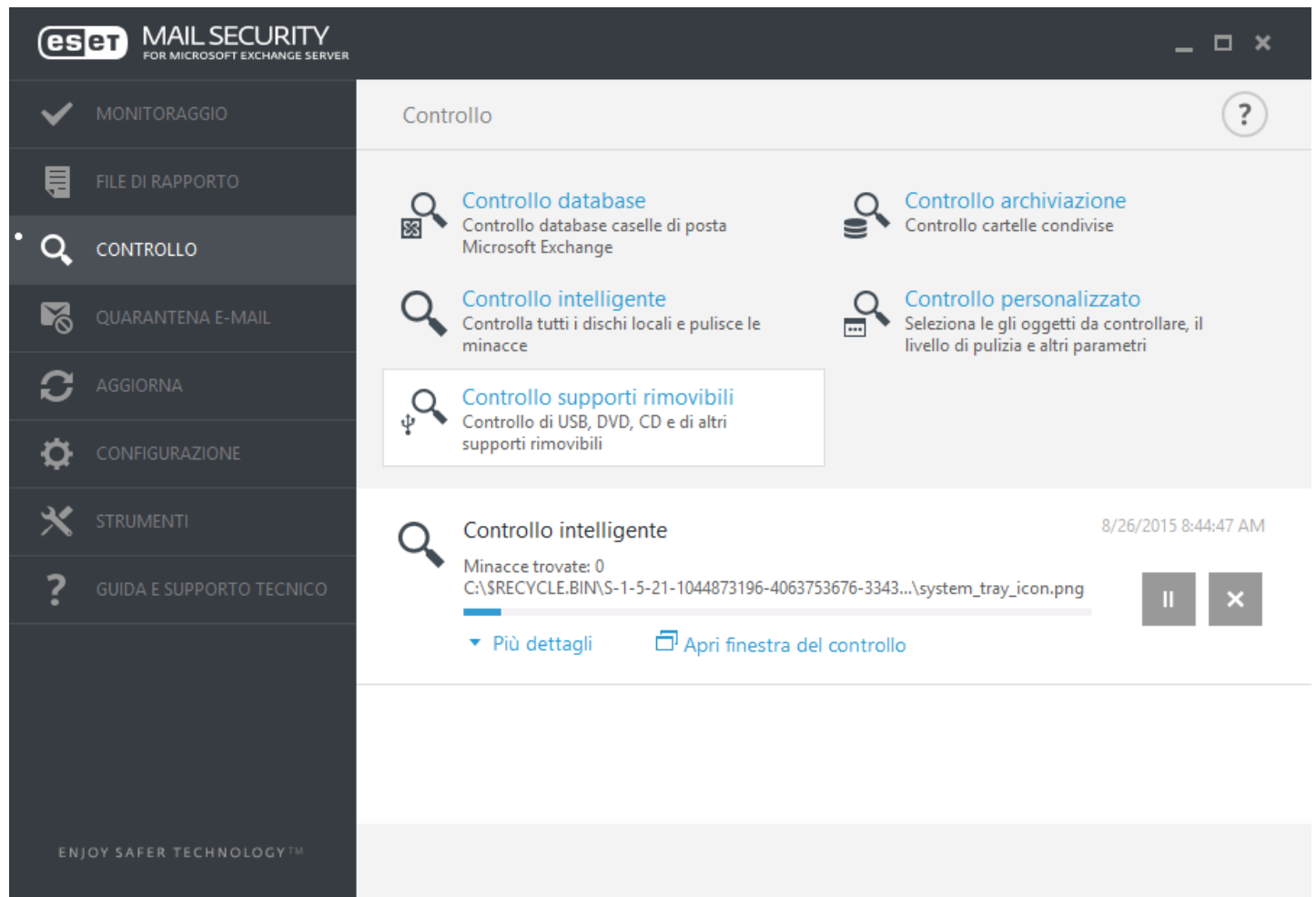
Fare clic su **Salva** per salvare le modifiche apportate alle selezioni di destinazioni, comprese quelle relative alla struttura delle cartelle.

Fare clic su **Controlla** per eseguire il controllo utilizzando i parametri personalizzati configurati dall'utente.

Effettua controllo come Amministratore consente di eseguire il controllo mediante l'account Amministratore. Selezionare questa opzione se l'utente corrente non dispone dei privilegi per accedere ai file appropriati da controllare. Nota: questo pulsante non è disponibile se l'utente corrente non può invocare operazioni UAC come Amministratore.

5.2.7.2 Avanzamento controllo

Nella finestra di avanzamento del controllo vengono mostrati lo stato attuale del controllo e informazioni sul numero di file rilevati che contengono codice dannoso.

NOTA: è normale che alcuni file, ad esempio file protetti con password o file che vengono utilizzati esclusivamente dal sistema (in genere il file *pagefile.sys* e alcuni file di registro), non possano essere sottoposti al controllo.

Avanzamento controllo: la barra di avanzamento mostra lo stato di oggetti già sottoposti al controllo rispetto a quelli in attesa. Lo stato di avanzamento del controllo viene ricavato dal numero totale di oggetti inclusi nel controllo.
Destinazione: nome dell'oggetto in fase di controllo e relativo percorso.
Minacce trovate: mostra il numero totale di minacce trovate durante un controllo.
Sospendi: sospende un controllo.
Riprendi: questa opzione è visibile quando l'avanzamento del controllo è sospeso. Fare clic su Riprendi per continuare il controllo.
Interrompi: interrompe il controllo.
Scorri rapporto di controllo: se questa opzione è attiva, il rapporto di controllo scorrerà automaticamente quando vengono aggiunte nuove voci in modo da rendere visibili le voci più recenti.

5.2.7.3 Gestione profili

La Gestione profili viene utilizzata in due modi all'interno di ESET Mail Security: nella sezione **Controllo computer su richiesta** e nella sezione **Aggiorna**.

Controllo del computer su richiesta

È possibile salvare i parametri di controllo preferiti per i controlli futuri. È consigliabile creare un profilo di controllo differente (con diverse destinazioni di controllo, metodi di controllo e altri parametri) per ciascun controllo utilizzato abitualmente.

Per creare un nuovo profilo, aprire la finestra Configurazione avanzata (F5) e fare clic su > **Controllo del computer su richiesta** quindi su **Modifica** accanto a **Elenco di profili**. Nel menu a discesa del **Profilo selezionato** sono elencati i profili di controllo esistenti. Per ricevere assistenza durante la creazione di un profilo di controllo adatto alle proprie esigenze, consultare la sezione Configurazione parametri motore ThreatSense contenente una descrizione di ciascun parametro di configurazione del controllo.

Esempio: si supponga di voler creare il proprio profilo di controllo e che la configurazione del Controllo intelligente sia appropriata solo in parte, in quanto non si desidera eseguire il controllo di eseguibili compressi o di applicazioni

potenzialmente pericolose e si intende applicare l'opzione **Massima pulizia**. Inserire il nome del nuovo profilo nella finestra **Gestione profili** e fare clic su **Aggiungi**. Selezionare il nuovo profilo dal menu a discesa **Profilo selezionato**, modificare i parametri rimanenti in base alle proprie esigenze e fare clic su **OK** per salvare il nuovo profilo.

Aggiornamento

L'editor dei profili nella sezione Impostazione aggiornamento consente agli utenti di creare nuovi profili di aggiornamento. Creare e utilizzare i profili personalizzati (diversi dal **Profilo personale** predefinito) solo se il computer utilizza vari metodi di connessione ai server di aggiornamento.

Ad esempio, un computer portatile che si connette normalmente a un server locale (mirror) nella rete locale ma scarica gli aggiornamenti direttamente dai server di aggiornamento ESET durante la disconnessione (trasferta di lavoro) potrebbe utilizzare due profili: il primo per connettersi al server locale e il secondo per connettersi ai server ESET. Dopo aver configurato questi profili, accedere a **Strumenti** > **Pianificazione attività** e modificare i parametri delle attività di aggiornamento. Indicare un profilo come principale e l'altro come secondario.

Profilo selezionato: profilo di aggiornamento attualmente utilizzato. Per modificarlo, scegliere un profilo dal menu a discesa.

Elenco di profili: crea nuovi profili di aggiornamento o modifica quelli esistenti.

5.2.7.4 Destinazioni di controllo

La finestra destinazioni di controllo consente all'utente di definire gli oggetti (memoria, unità, settori, file e cartelle) sui quali verranno ricercate le infiltrazioni. Selezionare gli oggetti dalla struttura ad albero contenente un elenco di tutti i supporti disponibili nel computer. Il menu a discesa **Destinazioni di controllo** consente di selezionare gli oggetti da controllare predefiniti.

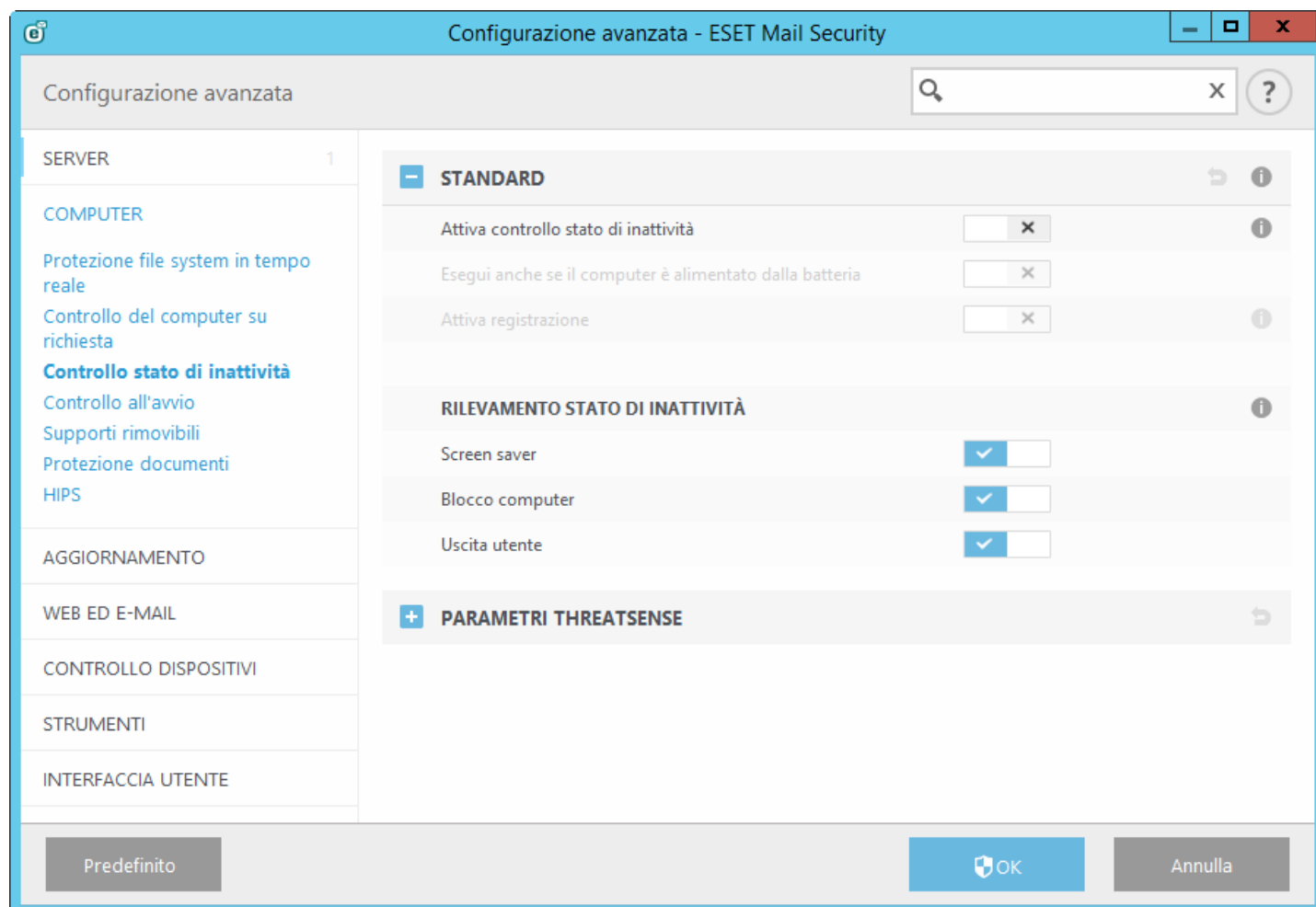
- **Attraverso le impostazioni di profilo**: consente di selezionare le destinazioni nel profilo di controllo selezionato.
- **Supporti rimovibili**: consente di selezionare dischi, supporti di archiviazione USB, CD/DVD.
- **Unità locali**: consente di selezionare tutti gli hard disk del sistema.
- **Unità di rete**: consente di selezionare tutte le unità di rete mappate.
- **Cartelle condivise**: consente di selezionare tutte le cartelle condivise sul server locale.
- **Nessuna selezione**: consente di annullare tutte le selezioni.

5.2.7.5 Sospendi un controllo pianificato

Il controllo pianificato può essere rimandato. Se si desidera rimandare il controllo del computer, definire un valore per l'opzione**Interrompi controlli pianificati in (min.)**.

5.2.8 Controllo stato di inattività

È possibile attivare lo scanner dello stato di inattività in **Configurazione avanzata** in > **Controllo stato di inattività** > **Di base**. Impostare il pulsante accanto a **Attiva controllo stato inattivo** su "On" per attivare questa funzionalità. Se il computer si trova nello stato di inattività, verrà eseguito un controllo silenzioso di tutti i dischi locali.

Per impostazione predefinita, lo scanner dello stato di inattività non verrà eseguito in caso di alimentazione del computer (notebook) a batteria. È possibile ignorare questa impostazione selezionando la casella di controllo accanto a **Esegui anche se il computer è alimentato a batteria** in Configurazione avanzata.

Attivare il pulsante **Attiva registrazione** in Configurazione avanzata per registrare il risultato di un controllo del computer nella sezione File di rapporto (nella finestra principale del programma, fare clic su **Strumenti** > **File di rapporto** e selezionare **Controllo del computer** dal menu a discesa **Rapporto**).

Il rilevamento dello stato di inattività verrà eseguito se il computer si trova nei seguenti stati:

- Screen saver
- Blocco computer
- Uscita utente

Fare clic su Parametri ThreatSense per modificare i parametri di controllo (ad esempio, metodi di rilevamento) per il controllo dello stato di inattività.

5.2.9 Controllo all'avvio

Per impostazione predefinita, all'avvio del sistema e durante gli aggiornamenti del database delle firme antivirali, verrà eseguito il controllo automatico del file di avvio. Questo controllo è gestito dalla Configurazione e attività Pianificazione attività.

Le opzioni di controllo all'avvio fanno parte della pianificazione dell'attività **Controllo del file di avvio del sistema**. Per modificare le impostazioni di controllo all'avvio, accedere a **Strumenti** > **Pianificazione attività**, fare clic su **Controllo automatico file di avvio**, quindi su **Modifica**. Nell'ultimo passaggio verrà visualizzata la finestra Controllo automatico file di avvio (per ulteriori informazioni, consultare il capitolo seguente).

Per ulteriori informazioni sulla creazione e sulla gestione di Pianificazione attività, consultare Creazione di nuove attività.

5.2.9.1 Controllo automatico file di avvio

Durante la creazione di un'attività pianificata di controllo del file di avvio del sistema, sono disponibili varie opzioni per regolare i parametri che seguono:

Il menu a discesa **Livello di controllo** consente di specificare il livello di controllo dei file eseguiti all'avvio del sistema. I file sono visualizzati in ordine crescente in base ai seguenti criteri:

- **Solo i file utilizzati più di frequente** (ultimi file sottoposti al controllo)
- **File utilizzati di frequente**
- **File utilizzati comunemente**
- **File utilizzati raramente**
- **Tutti i file registrati** (la maggior parte dei file sottoposti al controllo)

Sono inoltre inclusi due gruppi del **Livello di controllo** specifici:

- **File eseguiti prima dell'accesso utente**: contiene file da posizioni a cui è possibile accedere senza che l'utente abbia eseguito la registrazione (include quasi tutte le posizioni di avvio quali servizi, oggetti browser helper, notifiche Winlogon, voci della pianificazione attività di Windows, dll noti e così via).
- **File eseguiti dopo l'accesso utente**: contiene file da posizioni a cui è possibile accedere solo dopo che un utente ha eseguito la registrazione (include file che sono eseguiti solo per un utente specifico, in genere i file in *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Per ogni gruppo summenzionato, vengono definiti elenchi di file da sottoporre al controllo.

Priorità di controllo: livello di priorità utilizzato per determinare il momento di avvio di un controllo:

- **Normale** (con un carico di sistema medio),
- **Basso** (con un carico di sistema basso),
- **Più basso** (quando il carico di sistema è il più basso possibile),
- **Quando inattivo** (l'attività verrà eseguita solo quando il sistema è inattivo).

5.2.10 Supporti rimovibili

ESET Mail Security offre il controllo automatico dei supporti rimovibili (CD/DVD/USB). Questo modulo consente di controllare i supporti inseriti. Questa funzionalità può essere utile se l'amministratore del computer desidera impedire l'utilizzo di supporti rimovibili con contenuti non desiderati da parte degli utenti.

Azione da eseguire all'inserimento dei supporti rimovibili: selezionare l'azione predefinita che verrà eseguita quando un supporto rimovibile viene inserito nel computer (CD/DVD/USB). Selezionando **Mostra opzioni di controllo**, verrà visualizzata una notifica che consente all'utente di scegliere un'azione desiderata:

- **Non controllare**: non verrà eseguita alcuna azione e la finestra **Rilevato nuovo dispositivo** verrà chiusa.
- **Controllo automatico del dispositivo**: viene eseguito il controllo del computer su richiesta del supporto rimovibile inserito.
- **Mostra opzioni di controllo**: apre la sezione di configurazione dei supporti rimovibili.

All'inserimento di un supporto rimovibile, viene visualizzata la seguente finestra di dialogo:

- **Controlla ora**: avvia il controllo del supporto rimovibile.
- **Controlla più tardi**: il controllo del supporto rimovibile verrà posticipato.
- **Configurazione**: apre la Configurazione avanzata.
- **Usa sempre l'opzione selezionata**: se l'opzione è selezionata, verrà eseguita la stessa azione quando viene inserito nuovamente un supporto rimovibile.

In ESET Mail Security è inoltre disponibile la funzionalità Controllo dispositivi che consente all'utente di definire regole per l'utilizzo dei dispositivi esterni su un determinato computer. Per ulteriori informazioni sul Controllo dispositivi, consultare il paragrafo Controllo dispositivi.

5.2.11 Protezione documenti

La funzione Protezione documenti consente di eseguire il controllo dei documenti di Microsoft Office prima della loro apertura e dei file scaricati automaticamente da Internet Explorer, ad esempio gli elementi di Microsoft ActiveX. La funzione Protezione documenti offre un livello di protezione aggiuntivo rispetto alla protezione file system in tempo reale e può essere disattivata per ottimizzare le prestazioni di sistemi non esposti a volumi elevati di documenti Microsoft Office.

- **Integrazione nel sistema** consente di attivare il sistema di protezione. Per modificare questa opzione, premere F5 per aprire la finestra Configurazione avanzata e fare clic su > **Protezione documenti** nella struttura Configurazione avanzata.

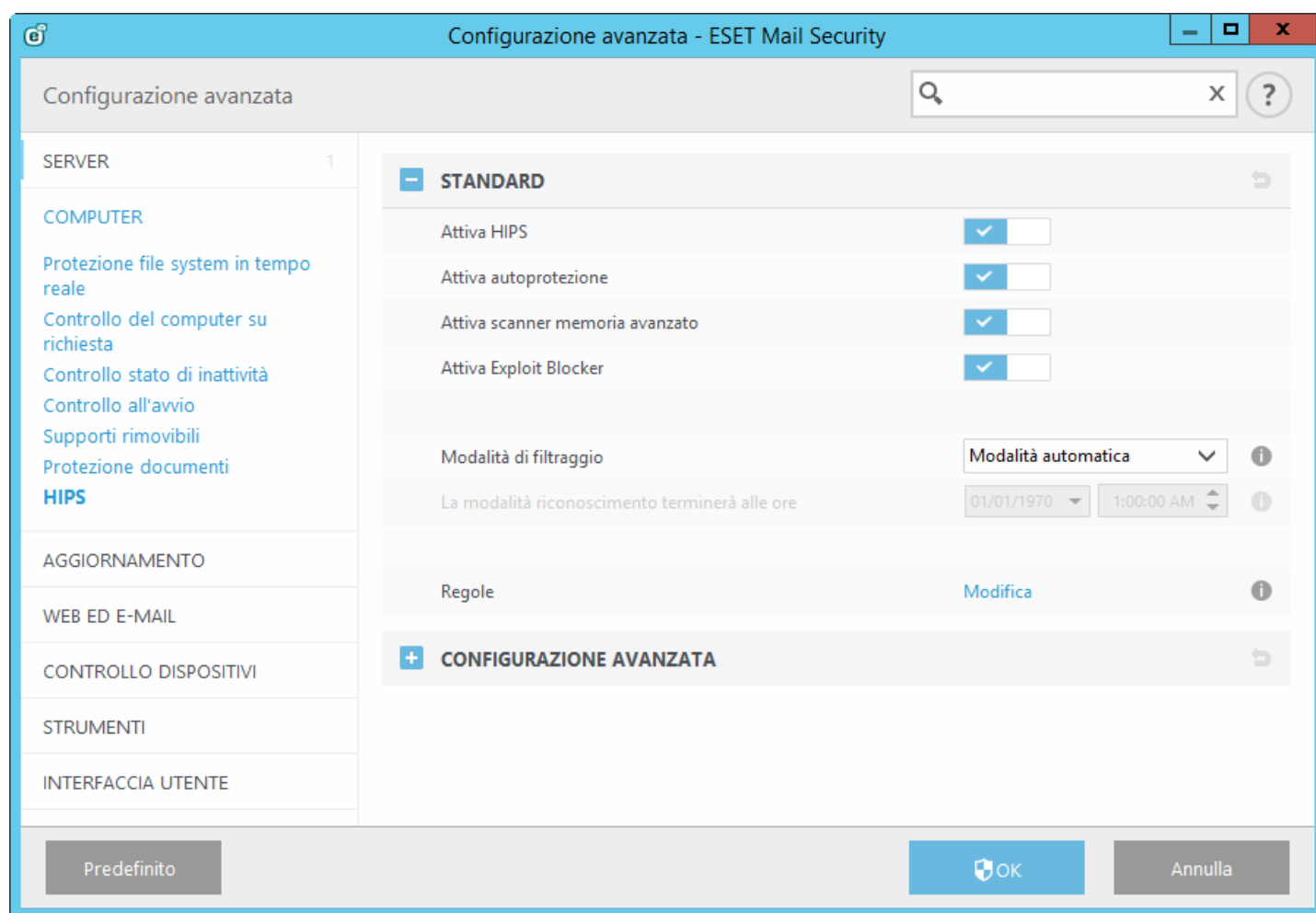
- Consultare Parametri Threatsense per ulteriori informazioni sulle impostazioni della protezione documenti.

Questa funzione è attivata dalle applicazioni che utilizzano Microsoft Antivirus API (ad esempio, Microsoft Office 2000 e versioni successive o Microsoft Internet Explorer 5.0 e versioni successive).

5.2.12 HIPS

È consigliabile che le modifiche delle impostazioni HIPS siano apportate solo dagli utenti avanzati. Una configurazione non corretta delle impostazioni HIPS può causare instabilità di sistema.

Il **Sistema anti-intrusione basato su host** (HIPS) protegge il sistema da malware o attività indesiderate che tentano di compromettere la sicurezza del computer. L'HIPS utilizza un'analisi comportamentale avanzata unita alle capacità di rilevamento del filtraggio di rete per il monitoraggio dei processi in esecuzione, dei file e delle chiavi del registro. L'HIPS è indipendente dalla protezione file system in tempo reale e non è un firewall, in quanto monitora solo i processi eseguiti all'interno del sistema operativo.

Le impostazioni dell'HIPS sono disponibili in **Configurazione avanzata** (F5) > > **HIPS**. Lo stato HIPS (attivato/disattivato) viene visualizzato nella finestra principale del programma ESET Mail Security, nel riquadro **Configurazione**, a destra della sezione **Computer**.

ESET Mail Security integra una tecnologia di *Autoprotezione* che impedisce a software dannosi di danneggiare o disattivare la protezione antivirus e antispyware, in modo da garantire costantemente la protezione del sistema. Le modifiche alle impostazioni **Attiva HIPS** e **Attiva autoprotezione** avranno effetto solo dopo aver riavviato il sistema operativo Windows. Sarà necessario riavviare il computer anche se si disattiva l'intero sistema **HIPS**.

Lo **Scanner memoria avanzato** lavora congiuntamente all'Exploit Blocker per rafforzare il livello di protezione contro malware concepiti allo scopo di eludere il rilevamento dei prodotti antimalware mediante l'utilizzo di pratiche di offuscamento o crittografia. Per impostazione predefinita, lo scanner memoria avanzato è attivo. Per ulteriori informazioni su questo tipo di protezione, consultare il glossario.

L'**Exploit Blocker** è progettato per rafforzare i tipi di applicazione comunemente utilizzati come browser Web, lettori PDF, client di posta e componenti di MS Office. L'exploit blocker è attivato per impostazione predefinita. Per ulteriori informazioni su questo tipo di protezione, consultare il glossario.

Il filtraggio può essere eseguito in una delle quattro seguenti modalità:

- **Modalità automatica**: le operazioni sono attivate, ad eccezione di quelle bloccate dalle regole predefinite che proteggono il sistema.
- **Modalità intelligente**: all'utente verranno segnalati solo gli eventi molto sospetti.
- **Modalità interattiva**: all'utente verrà chiesto di confermare le operazioni.
- **Modalità basata su criteri**: le operazioni sono bloccate.
- **Modalità riconoscimento**: le operazioni sono attivate e dopo ogni operazione viene creata una regola. Le regole create in questa modalità possono essere visualizzate nell'Editor regole, ma la loro priorità è inferiore rispetto alla priorità delle regole create manualmente o delle regole create nella modalità automatica. Selezionando la Modalità riconoscimento dal menu a discesa Modalità filtraggio HIPS, sarà disponibile l'impostazione La modalità riconoscimento terminerà alle ore. Selezionare la durata per la quale si desidera attivare la modalità riconoscimento (il limite massimo è di 14 giorni). Una volta trascorsa la durata specificata, all'utente verrà richiesto di modificare le regole create dall'HIPS quando si trovava in modalità riconoscimento. È inoltre possibile scegliere un'altra modalità di filtraggio oppure posticipare la decisione e continuare a utilizzare la modalità riconoscimento.

Il sistema HIPS monitora gli eventi all'interno del sistema operativo e reagisce in base a regole simili a quelle utilizzate dal rapporto del Personal firewall. Fare clic su **Modifica** per aprire la finestra di gestione delle regole HIPS. In questa sezione è possibile selezionare, creare, modificare o eliminare regole. Per ulteriori informazioni sulla creazione delle regole e sulle operazioni HIPS, consultare il capitolo Modifica regola.

Se l'azione predefinita di una regola è impostata su Chiedi, verrà visualizzata una finestra di dialogo tutte le volte che la regola verrà attivata. È possibile scegliere di **Bloccare** o **Consentire** l'operazione. Se l'utente non sceglie un'azione nell'intervallo di tempo specifico, verrà selezionata una nuova azione in base alle regole.

La finestra di dialogo consente all'utente di creare una regola in base a una qualsiasi nuova azione rilevata dall'HIPS e di definire le condizioni in base alle quali consentire o bloccare l'azione. Per accedere ai parametri corretti, fare clic su **Mostra opzioni**. Le regole create in questo modo sono considerate equivalenti a quelle create manualmente. Una regola creata da una finestra di dialogo può quindi essere meno specifica rispetto alla regola che ha attivato quella finestra di dialogo. Ciò significa che, dopo aver creato questo tipo di regola, la stessa operazione può attivare la stessa finestra.

Ricorda temporaneamente questa azione per il processo causa un'azione (**Consenti/Blocca**) da utilizzare finché non verrà apportata una modifica alle regole o alla modalità di filtraggio oppure non verrà eseguito un aggiornamento del modulo HIPS o un riavvio del sistema. In seguito a una di queste tre azioni, le regole temporanee verranno eliminate.

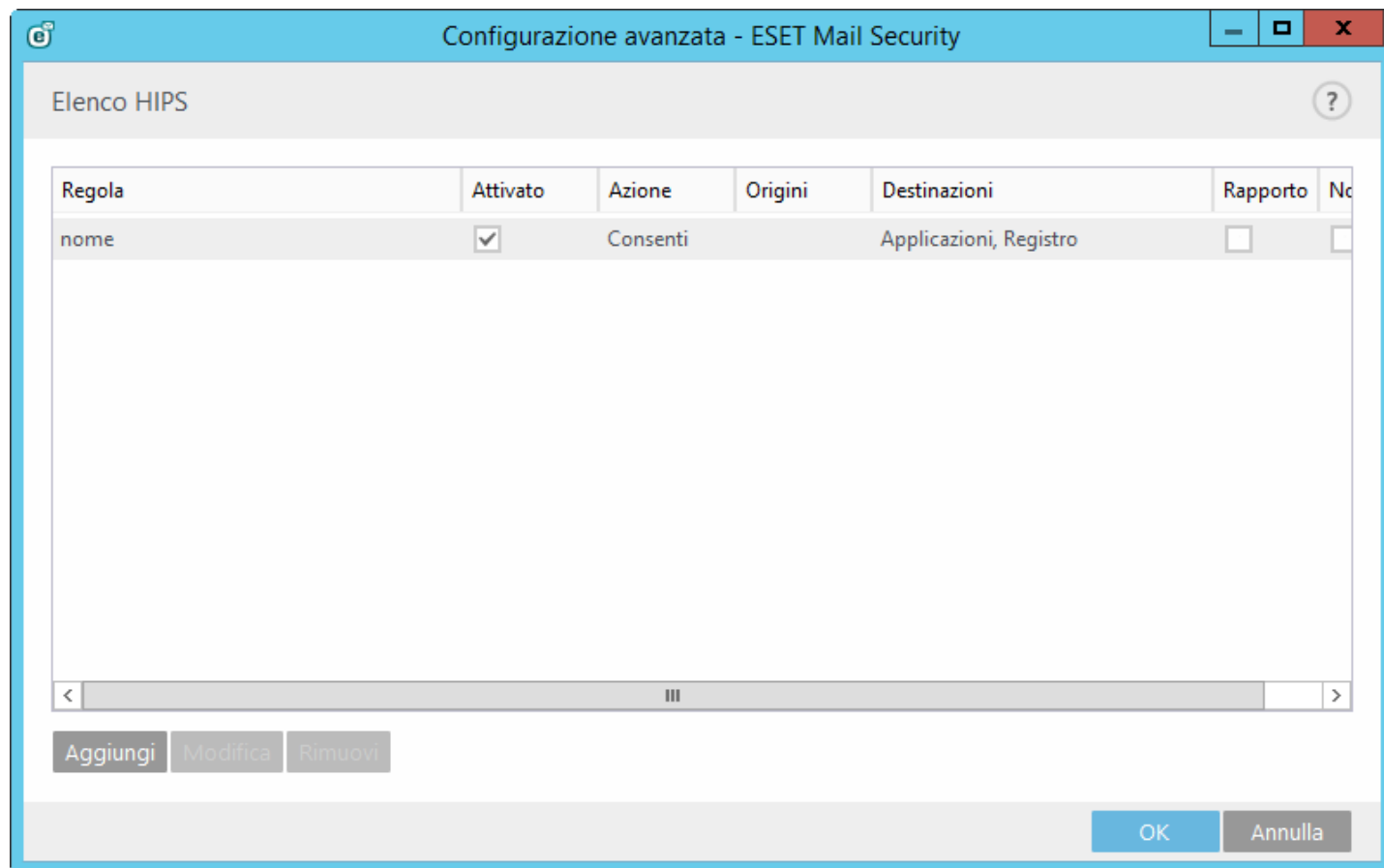
5.2.12.1 Regole HIPS

La finestra offre una panoramica delle regole HIPS esistenti.

Colonne

Regola: nome della regola scelto automaticamente o definito dall'utente.
Attivata: disattivare questo pulsante se si desidera mantenere la regola nell'elenco ma non si desidera utilizzarla.
Azione: la regola specifica un'azione - **Consenti**, **Blocca** o **Chiedi** - che deve essere eseguita se sono soddisfatte le condizioni specificate.
Origini: la regola verrà utilizzata solo se l'evento viene attivato da una o più applicazioni.
Destinazioni: la regola verrà utilizzata esclusivamente se l'operazione è correlata a un file, un'applicazione o una voce di registro specifici.
Rapporto: se si attiva questa opzione, le informazioni sulla regola verranno scritte nel Rapporto HIPS.
Notifica: se viene attivato un evento, nell'angolo in basso a destra viene visualizzata una finestra popup di piccole dimensioni.

Elementi di controllo

Aggiungi: crea una nuova regola.
Modifica: consente all'utente di modificare le voci selezionate.
Rimuovi: rimuove le voci selezionate.

5.2.12.1.1 Impostazioni regole HIPS

- **Nome regola**: nome della regola scelto automaticamente o definito dall'utente.
- **Azione**: la regola specifica un'azione - **Consenti**, **Blocca** o **Chiedi** - che deve essere eseguita se sono soddisfatte le condizioni specificate.
- **Operazioni che influiscono**: è necessario selezionare il tipo di operazione alla quale la regola verrà applicata. La regola verrà utilizzata solo per questo tipo di operazione e per la destinazione selezionata.
- **File**: la regola verrà utilizzata solo se l'operazione è correlata a questa destinazione. Selezionare File specifici dal menu a discesa e fare clic su Aggiungi per aggiungere nuovi file o cartelle oppure selezionare Tutti i file dal menu a discesa per aggiungere tutte le applicazioni.
- **Applicazioni**: la regola verrà utilizzata solo se l'evento viene attivato dall'applicazione. Selezionare Applicazioni specifiche dal menu a discesa e fare clic su Aggiungi per aggiungere nuovi file o cartelle oppure selezionare Tutte le applicazioni dal menu a discesa per aggiungere tutte le applicazioni.
- **Voci di registro**: la regola verrà utilizzata solo se l'operazione è correlata a questa destinazione. Selezionare Voci specifiche dal menu a discesa e fare clic su Aggiungi per aggiungere nuovi file o cartelle oppure selezionare Tutte le voci dal menu a discesa per aggiungere tutte le applicazioni.
- **Attivata**: disattivare questo pulsante se si desidera mantenere la regola nell'elenco senza utilizzarla.
- **Rapporto**: se si attiva questa opzione, le informazioni sulla regola verranno scritte nel Rapporto HIPS.
- **Notifica utente**: se viene attivato un evento, nell'angolo in basso a destra viene visualizzata una finestra popup di piccole dimensioni.

La regola è formata da varie parti che illustrano le condizioni che la attivano:

Applicazioni di origine: la regola verrà utilizzata solo se l'evento viene attivato dall'applicazione. Selezionare **Applicazioni specifiche** dal menu a discesa e fare clic su **Aggiungi** per aggiungere nuovi file o cartelle oppure selezionare **Tutte le applicazioni** dal menu a discesa per aggiungere tutte le applicazioni.

File: la regola verrà utilizzata solo se l'operazione è correlata a questa destinazione. Selezionare **File specifici** dal menu a discesa e fare clic su **Aggiungi** per aggiungere nuovi file o cartelle oppure selezionare **Tutti i file** dal menu a discesa per aggiungere tutte le applicazioni.

Applicazioni : la regola verrà utilizzata solo se l'operazione è correlata a questa destinazione. Selezionare **Applicazioni specifiche** dal menu a discesa e fare clic su **Aggiungi** per aggiungere nuovi file o cartelle oppure selezionare **Tutte le applicazioni** dal menu a discesa per aggiungere tutte le applicazioni.

Voci di registro: la regola verrà utilizzata solo se l'operazione è correlata a questa destinazione. Selezionare **Voci specifiche** dal menu a discesa e fare clic su **Aggiungi** per aggiungere nuovi file o cartelle oppure selezionare **Tutte le voci** dal menu a discesa per aggiungere tutte le applicazioni.

Descrizione delle operazioni importanti:

Operazioni del file

- **Elimina file**: l'applicazione richiede l'autorizzazione per l'eliminazione del file di destinazione.
- **Scrivi su file**: l'applicazione richiede l'autorizzazione per scrivere sul file di destinazione.
- **Accesso diretto al disco**: l'applicazione sta tentando di leggere o scrivere sul disco in modalità non standard, che eluderà le procedure di Windows comuni. Ciò potrebbe causare la modifica dei file senza che vengano applicate le regole corrispondenti. Questa operazione può essere causata da un malware che tenta di eludere il rilevamento, un software di backup che tenta di creare una copia esatta di un disco o un programma di gestione delle partizioni che tenta di riorganizzare i volumi del disco.
- **Installa hook globale**: fa riferimento alla chiamata della funzione SetWindowsHookEx dalla libreria MSDN.
- **Carica driver**: installazione e caricamento dei driver nel sistema.

Operazioni dell'applicazione

- **Esegui debug di un'altra applicazione**: associazione di un debugger al processo. Quando si esegue il debug di un'applicazione, è possibile visualizzare e modificare molti dettagli del relativo comportamento e accedere ai rispettivi dati.
- **Intercetta eventi da altra applicazione**: l'applicazione di origine sta tentando di intercettare gli eventi specifici su un'applicazione specifica (ad esempio, un keylogger che cerca di acquisire gli eventi del browser).
- **Termina/sospendi altra applicazione**: sospensione, ripresa o interruzione di un processo (è possibile accedervi direttamente da Process Explorer o dal riquadro Processi).
- **Avvia nuova applicazione**: avvio di nuove applicazioni o processi.
- **Modifica stato di un'altra applicazione**: l'applicazione di origine sta tentando di scrivere nella memoria delle applicazioni di destinazione o di eseguire codice per suo conto. Questa funzionalità può risultare utile per proteggere un'applicazione essenziale configurandola come applicazione di destinazione in una regola che blocca l'utilizzo di tale operazione.

Operazioni del registro

- **Modifica impostazioni di avvio**: qualsiasi modifica nelle impostazioni che definisce quali applicazioni saranno eseguite all'avvio di Windows. Possono essere individuate, ad esempio, ricercando la chiave Run nel Registro di sistema di Windows.
- **Elimina dal registro**: eliminazione di una chiave del registro o del relativo valore.
- **Rinomina chiave del registro**: ridenominazione delle chiavi del registro.
- **Modifica registro**: creazione di nuovi valori delle chiavi del registro, modifica dei valori esistenti, spostamento dei dati nella struttura del database oppure impostazione dei diritti utente o di gruppo per le chiavi del registro.

i **NOTA:** quando si inserisce una destinazione, è possibile utilizzare i caratteri jolly con alcune limitazioni. Al posto di una chiave particolare, nei percorsi dei registri di sistema è possibile utilizzare il simbolo * (asterisco). Ad esempio, *HKEY_USERS*\software* può significare *HKEY_USER\.default\software* ma non *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** non è un percorso valido della chiave di registro del sistema. Un percorso della chiave del registro di sistema contenente *

indica "questo percorso o qualsiasi percorso a qualsiasi livello dopo tale simbolo". Nelle destinazioni dei file, i caratteri jolly possono essere utilizzati solo in questo modo. Viene innanzitutto valutata la parte specifica di un percorso, quindi viene esaminato il percorso dopo il carattere jolly (*).

 In caso di creazione di una regola molto generica, verrà visualizzato un avviso su questo tipo di regola.

Nell'esempio seguente viene spiegato come limitare il comportamento indesiderato delle applicazioni:

5.2.12.2 Configurazione avanzata

Le seguenti opzioni sono utili per eseguire il debug e l'analisi del comportamento di un'applicazione:

Caricamento driver sempre consentito: i driver selezionati sono sempre autorizzati a caricare indipendentemente dalla modalità di filtraggio configurata, eccetto nel caso in cui vengano bloccati esplicitamente da una regola dell'utente.

Registra tutte le operazioni bloccate: tutte le operazioni bloccate verranno scritte sul registro HIPS.

Notifica quando si verificano modifiche nelle applicazioni all'Avvio: consente di visualizzare una notifica sul desktop ogni volta che un'applicazione viene aggiunta o rimossa dall'avvio del sistema.

Per una versione aggiornata di questa pagina della Guida, consultare l'articolo della Knowledge Base.

5.2.12.2.1 Caricamento driver sempre consentito

I driver visualizzati in questo elenco sono sempre autorizzati a caricare indipendentemente dalla modalità di filtraggio dell'HIPS, eccetto nel caso in cui vengano bloccati esplicitamente da una regola dell'utente.

Aggiungi: aggiunge un nuovo driver.
Modifica: modifica il percorso di un driver selezionato.
Rimuovi: rimuove un driver dall'elenco.
Reimposta: ricarica un set di driver di sistema.

i **NOTA:** fare clic su **Reimposta** se non si desidera includere i driver aggiunti manualmente. Questa funzione può rivelarsi utile nel caso in cui l'utente abbia aggiunto vari driver e non possa eliminarli manualmente dall'elenco.

5.3 Aggiornamento

Le opzioni di configurazione degli aggiornamenti sono disponibili nella struttura **Configurazione avanzata** (F5) in **Aggiornamento** > **Generale**. Questa sezione consente di specificare informazioni sull'origine degli aggiornamenti, come ad esempio i server di aggiornamento e i dati per l'autenticazione di tali server.

Generale

Il profilo di aggiornamento attualmente in uso viene visualizzato nel menu a discesa **Profilo selezionato**. Per creare un nuovo profilo, fare clic su **Modifica** accanto a **Elenco di profili**, inserire il proprio **Nome profilo**, quindi fare clic su **Aggiungi**.

In caso di problemi con un aggiornamento, fare clic su **Cancella** per eliminare la cache dei file di aggiornamento temporanei.

Avvisi database firme antivirali obsoleto

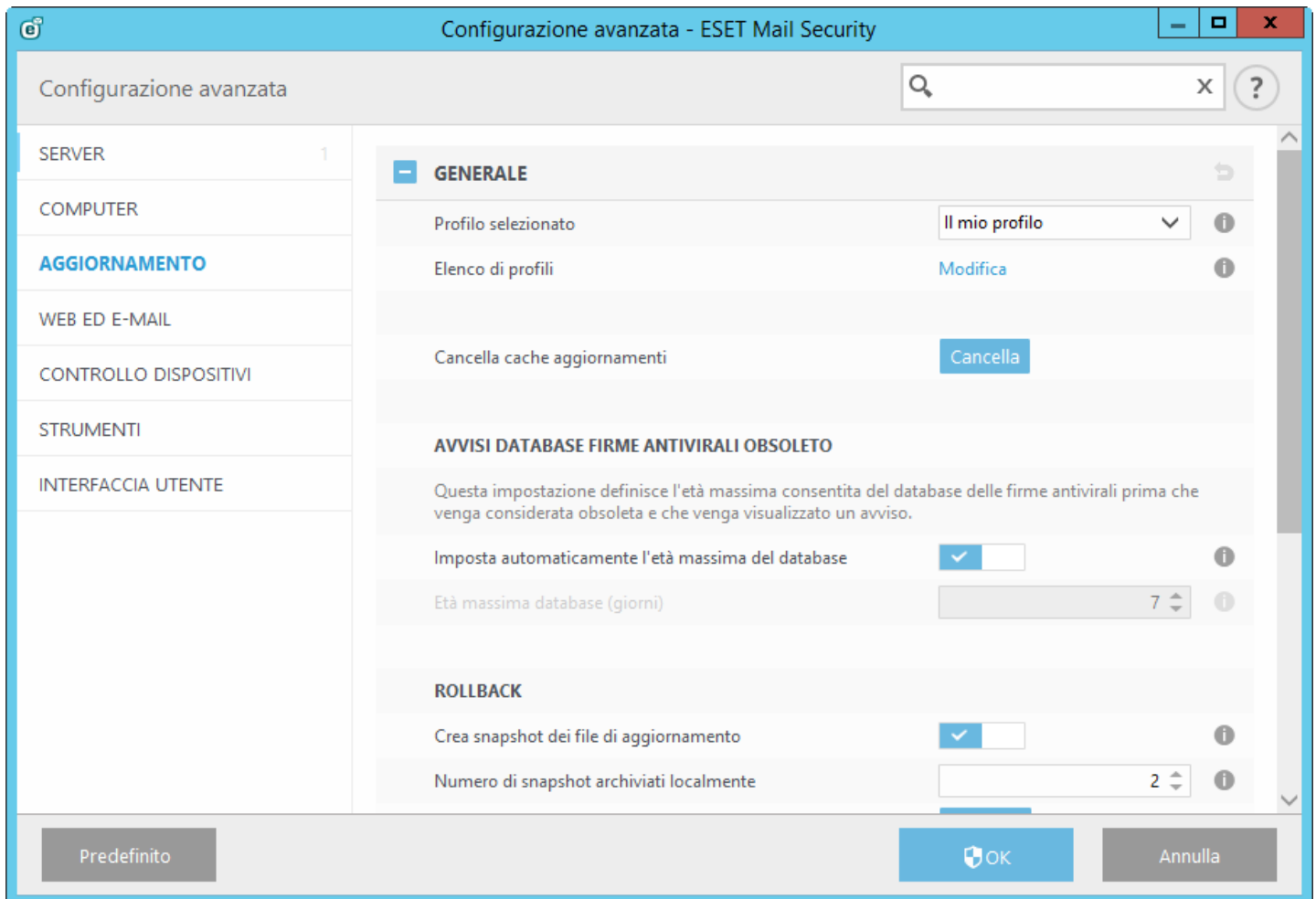
Imposta automaticamente l'età massima del database: consente di impostare il tempo massimo (in giorni) dopo il quale il database delle firme antivirali verrà segnalato come obsoleto. Il valore predefinito è 7.

Rollback

Se si sospetta che un nuovo aggiornamento del database delle firme antivirali e/o dei moduli del programma possa essere instabile o danneggiato, è possibile ripristinare la versione precedente e disattivare gli aggiornamenti per un determinato periodo di tempo. In alternativa, è possibile attivare gli aggiornamenti precedentemente disattivati in

caso di rimando indefinito da parte dell'utente.

ESET Mail Security registra gli snapshot del database delle firme antivirali e dei moduli del programma da utilizzare con la funzione *rollback*. Per creare snapshot del database delle firme antivirali, lasciare selezionato il pulsante **Crea snapshot dei file di aggiornamento**. Il campo **Numero di snapshot memorizzati localmente** definisce il numero di snapshot del database delle firme antivirali precedentemente archiviati.

Se si fa clic su **Rollback** (**Configurazione avanzata** (F5) > **Aggiorna** > **Generale**), è necessario scegliere un intervallo temporale dal menu a discesa che indica il periodo di tempo nel quale gli aggiornamenti del database delle firme antivirali e del modulo di programma verranno sospesi.

Per scaricare correttamente gli aggiornamenti, occorre inserire tutti i parametri di aggiornamento richiesti. Se si utilizza un firewall, assicurarsi che al programma ESET sia consentito di comunicare con Internet (ad esempio, comunicazione HTTP).

Per impostazione predefinita, il **Tipo di aggiornamento** (posizionato sotto a **Di base**) è impostato su **Aggiornamento periodico** per garantire che i file di aggiornamento vengano scaricati automaticamente dal server ESET che presenta il traffico di rete minore.

Di base

Disattiva visualizzazione notifiche relative agli aggiornamenti eseguiti correttamente: disattiva la notifica sulla barra delle applicazioni nell'angolo in basso a destra della schermata. È utile selezionare questa opzione se è in esecuzione un'applicazione a schermo intero o un videogioco. Tenere presente che la modalità presentazione disattiverà tutte le notifiche.

Per impostazione predefinita, il menu **Server di aggiornamento** è impostato su SELEZIONE AUTOMATICA. Il server di aggiornamento rappresenta il luogo di archiviazione degli aggiornamenti. Se si utilizza un server ESET, si consiglia di lasciare selezionata l'opzione predefinita. In caso di utilizzo del server di aggiornamento personalizzato e qualora si desideri ripristinare le impostazioni predefinite, digitare **SELEZIONE AUTOMATICA**. ESET Mail Security sceglierà automaticamente i server di aggiornamento ESET.

Quando si utilizza un server HTTP locale (noto anche come mirror), il server di aggiornamento deve essere impostato come riportato di seguito:
http://nome_computer_o_relativo_indirizzo_IP:2221

Quando si utilizza un server HTTP locale con SSL, il server di aggiornamento deve essere impostato come riportato di seguito:
https://nome_computer_o_relativo_indirizzo_IP:2221

Quando si utilizza una cartella locale condivisa, il server di aggiornamento deve essere impostato come riportato di seguito:
\\nome_computer__o_relativo_indirizzo_IP\cartella_condivisa

Aggiornamento dal mirror

L'autenticazione per i server di aggiornamento si basa sulla **Chiave di licenza** generata e inviata dopo l'acquisto. In caso di utilizzo di un server mirror locale, è possibile definire le credenziali per consentire ai client di accedere al server mirror prima di ricevere gli aggiornamenti. Per impostazione predefinita, non è richiesta alcuna verifica e i campi **Nome utente** e **Password** sono lasciati vuoti.

5.3.1 Rollback aggiornamento

Se si fa clic su **Rollback** (**Configurazione avanzata** (F5) > **Aggiornamento** > **Profilo**), è necessario scegliere un intervallo temporale dal menu a discesa che indica il periodo di tempo nel quale gli aggiornamenti del database delle firme antivirali e del modulo di programma verranno sospesi.

Selezionare **Fino a revoca** per rimandare in modo indefinito gli aggiornamenti periodici finché l'utente non avrà ripristinato la funzionalità degli aggiornamenti manualmente. Non è consigliabile selezionare questa opzione in quanto rappresenta un potenziale rischio per la protezione.

Il database delle firme antivirali viene ripristinato alla versione più vecchia disponibile e memorizzato come snapshot nel file system del computer locale.

Esempio: si supponga che la versione più recente del database delle firme antivirali corrisponde al numero 10646. Le versioni 10645 e 10643 sono memorizzate come snapshot del database delle firme antivirali. Si tenga presente che la versione 10644 non è disponibile poiché, ad esempio, il computer è stato spento ed è stato reso disponibile un aggiornamento più recente prima che venisse scaricata la versione 10644. Se il campo **Numero di snapshot memorizzati localmente** è impostato su 2 e si fa clic su **Rollback**, il database delle firme antivirali (compresi i moduli del programma) verrà ripristinato al numero di versione 10643. Il processo potrebbe richiedere alcuni minuti. Verificare se il database delle firme antivirali è stato ripristinato a una versione precedente dalla finestra principale del programma di ESET Mail Security nella sezione Aggiornamento.

5.3.2 Modalità di aggiornamento

La scheda **Modalità di aggiornamento** contiene opzioni correlate all'aggiornamento dei componenti di programma. Il programma consente di preimpostare le azioni da eseguire quando è disponibile un nuovo aggiornamento dei componenti di programma.

Gli aggiornamenti dei componenti di programma aggiungono nuove funzioni o introducono modifiche alle funzioni già esistenti nelle versioni precedenti. Possono essere eseguiti automaticamente senza alcun intervento da parte dell'utente oppure è possibile scegliere di ricevere una notifica. Una volta installato l'aggiornamento dei componenti di programma, potrebbe essere necessario riavviare il computer. Nella sezione **Aggiornamento componenti programma** sono disponibili tre opzioni:

- **Chiedi prima di scaricare i componenti di programma**: opzione predefinita. All'utente verrà chiesto di confermare o rifiutare gli aggiornamenti dei componenti di programma, se disponibili.
- **Aggiorna sempre i componenti di programma**: l'aggiornamento dei componenti di programma verrà scaricato e installato automaticamente. Ricordare che potrebbe essere necessario riavviare il computer.
- **Non aggiornare mai i componenti di programma**: l'aggiornamento dei componenti di programma non viene eseguito. Questa opzione è adatta alle installazioni su server, poiché di norma i server possono essere riavviati solo durante la manutenzione.

NOTA: la scelta dell'opzione più adatta dipende dalla workstation sulla quale saranno applicate le impostazioni. Tenere presente che esistono alcune differenze tra le workstation e i server. Ad esempio, il riavvio automatico del server dopo un aggiornamento di un programma potrebbe causare gravi danni.

Se è attiva l'opzione **Chiedi prima di scaricare l'aggiornamento**, verrà visualizzata una notifica ogni volta che è disponibile un nuovo aggiornamento.

Se la dimensione del file di aggiornamento supera il valore specificato nel campo **Chiedi se un file di aggiornamento è maggiore di (KB)**, verrà visualizzata una notifica.

5.3.3 Proxy HTTP

Per accedere alle opzioni di configurazione del server proxy per uno specifico profilo di aggiornamento, fare clic su **Aggiorna** nella struttura **Configurazione avanzata** (F5), quindi su **Proxy HTTP**. Fare clic sul menu a discesa **Modalità proxy** e selezionare una delle tre seguenti opzioni:

- Non utilizzare server proxy
- Connessione tramite server proxy
- Utilizza impostazioni server proxy globali

Se si seleziona l'opzione **Utilizza impostazioni server proxy globali**, verranno utilizzate le opzioni di configurazione del server proxy già specificate all'interno della sottostruttura **Strumenti** > **Server proxy** della struttura Configurazione avanzata.

Selezionare **Non utilizzare server proxy** per specificare che non verrà utilizzato alcun server proxy per l'aggiornamento di ESET Mail Security.

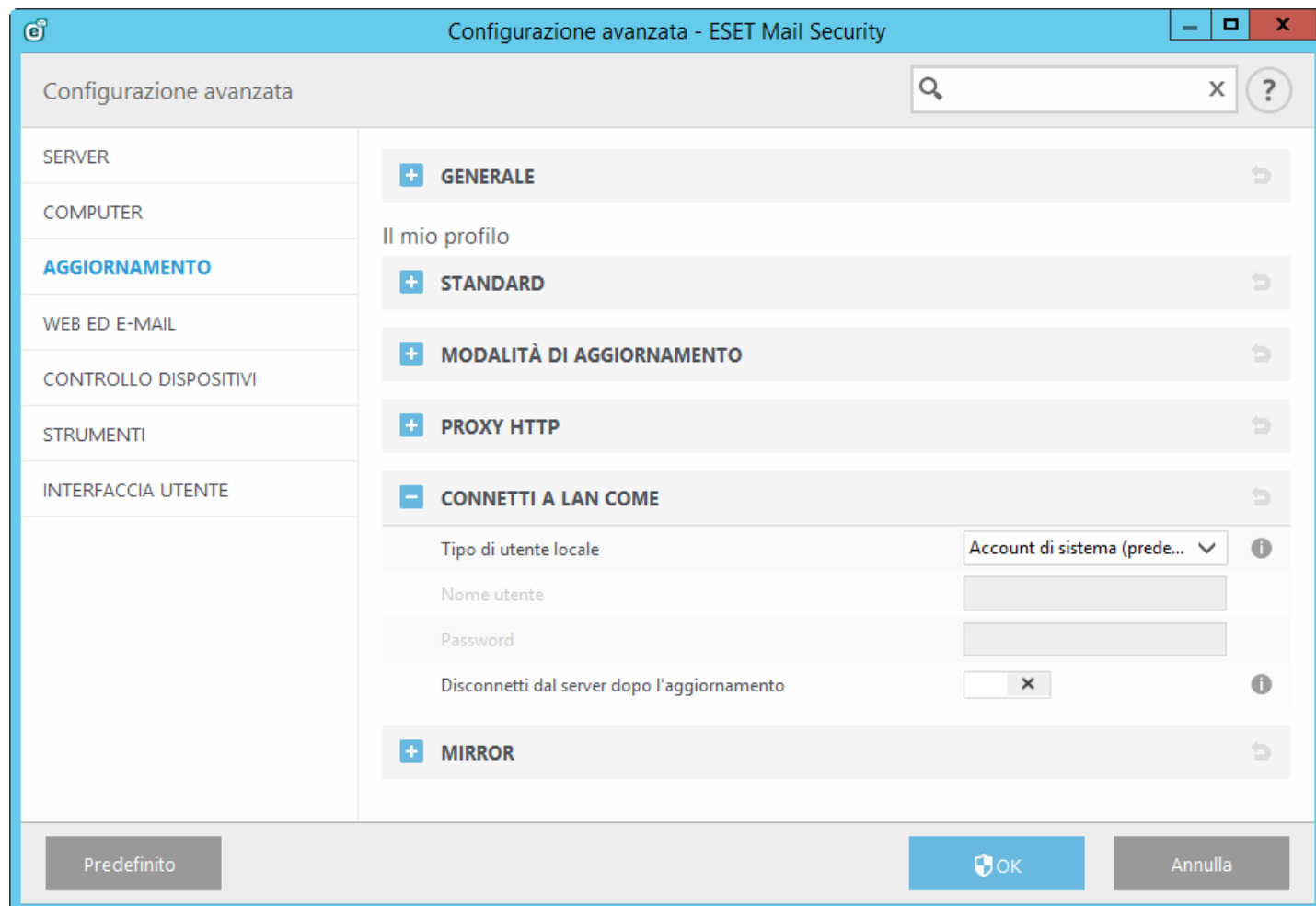
Selezionare l'opzione **Connessione tramite server proxy** nei seguenti casi:

- È necessario utilizzare un server proxy per aggiornare ESET Mail Security e tale server è differente da quello specificato nelle impostazioni globali (**Strumenti** > **Server proxy**). In questo caso, sarà necessario fornire alcune informazioni aggiuntive: Indirizzo del **Server proxy**, **Porta** di comunicazione (3128 per impostazione predefinita), più **Nome utente** e **Password** per il server del proxy, se necessario.
- Le impostazioni del server proxy non sono state configurate a livello globale. ESET Mail Security effettuerà tuttavia la connessione a un server proxy per verificare la disponibilità di aggiornamenti.
- Il computer è connesso a Internet tramite un server proxy. Le impostazioni vengono estrapolate da Internet Explorer durante l'installazione del programma. Tuttavia, in caso di modifiche successive, ad esempio, se si cambia il provider di servizi Internet (ISP), è necessario verificare che le impostazioni del proxy HTTP elencate in questa finestra siano corrette. In caso contrario, il programma non sarà in grado di connettersi ai server di aggiornamento.

L'impostazione predefinita per il server proxy è **Utilizza impostazioni server proxy globali**.

ℹ **NOTA:** i dati di autenticazione, come ad esempio il **Nome utente** e la **Password**, sono necessari per accedere al server proxy. Compilare questi campi solo se sono richiesti un nome utente e una password. Tenere presente che questi campi, in cui non è necessario inserire il nome utente e la password di ESET Mail Security, devono essere completati solo se è richiesta una password di accesso a Internet mediante un server proxy.

5.3.4 Connetti a LAN come

Durante l'aggiornamento da un server locale con una versione del sistema operativo Windows NT, per impostazione predefinita è richiesta l'autenticazione per ciascuna connessione di rete.

Per configurare un account simile, selezionare dal menu a discesa **Tipo di utente locale**:

- **Account di sistema (predefinito)**,
- **Utente corrente**,
- **Utente specificato**.

Selezionare **Account di sistema (predefinito)** per utilizzare l'account di sistema per l'autenticazione. In genere non viene eseguito alcun processo di autenticazione se nella sezione principale di impostazione dell'aggiornamento non sono specificati dati di autenticazione.

Per essere certi che il programma esegua l'autenticazione utilizzando l'account di un utente che ha eseguito correntemente l'accesso, selezionare **Utente corrente**. Lo svantaggio di questa soluzione consiste nel fatto che il programma non è in grado di connettersi al server di aggiornamento se nessun utente ha eseguito l'accesso in quel momento.

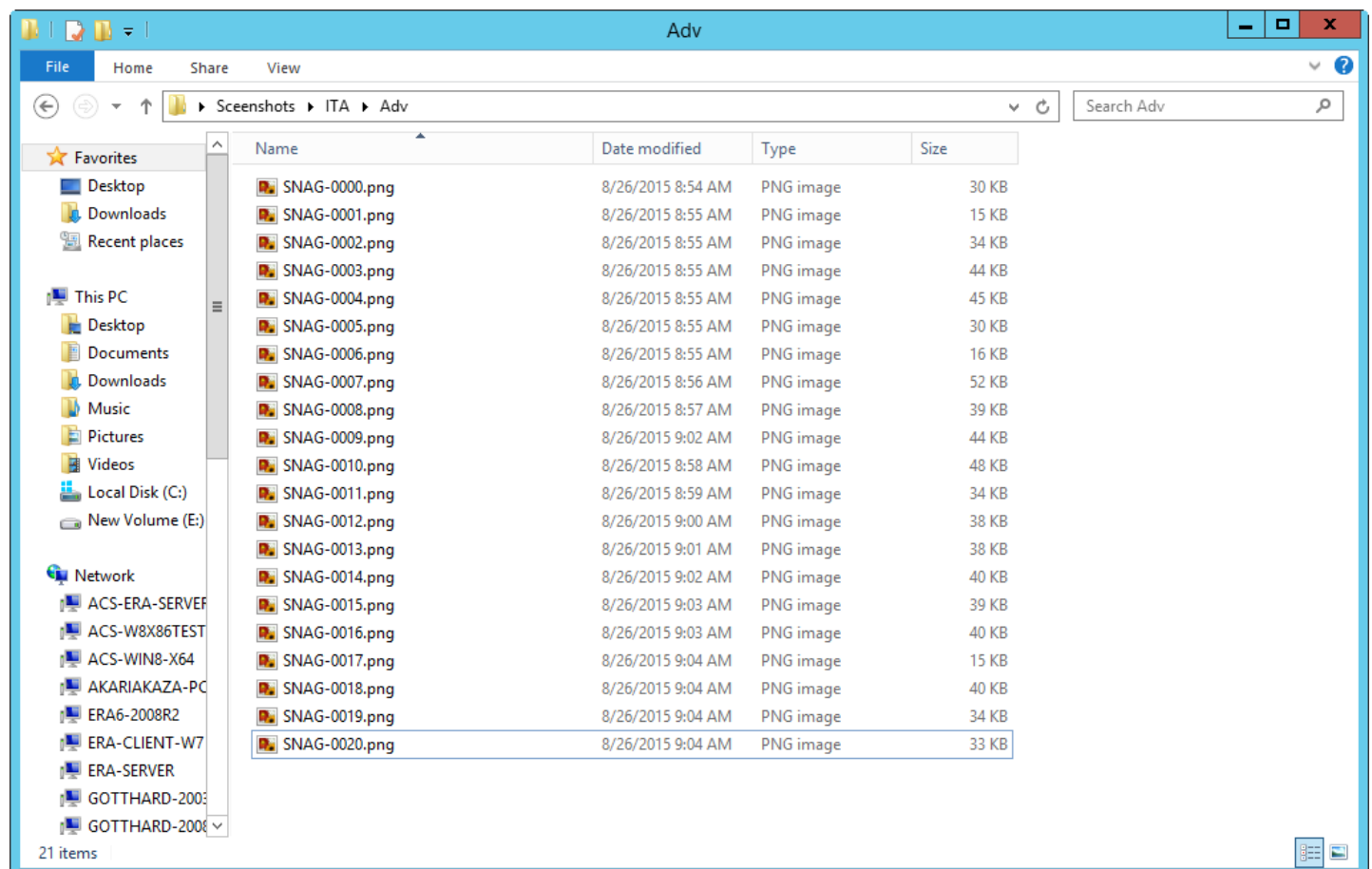
Selezionare **Utente specificato** se si desidera che il programma utilizzi un account utente specifico per l'autenticazione. Utilizzare questo metodo quando la connessione con l'account di sistema predefinito non riesce. Tenere presente che l'account dell'utente specificato deve disporre dell'accesso alla directory dei file di aggiornamento sul server locale. In caso contrario, il programma non sarà in grado di stabilire una connessione e scaricare gli aggiornamenti.

Avviso: se si seleziona **Utente corrente** o **Utente specificato**, è possibile che si verifichi un errore quando si modifica l'identità del programma per l'utente desiderato. È consigliabile immettere i dati di autenticazione della LAN nella sezione principale di configurazione dell'aggiornamento. In questa sezione di impostazione dell'aggiornamento, i dati di autenticazione devono essere inseriti come segue: *nome_dominio\utente* (se si tratta di un gruppo di lavoro, immettere *none_gruppodilavoro\nome*) e la password utente. Per l'aggiornamento dalla versione HTTP del server locale, non è richiesta alcuna autenticazione.

Attivare **Disconnetti dal server dopo l'aggiornamento** per forzare una disconnessione se una connessione al server dovesse rimanere attiva anche dopo il download degli aggiornamenti.

5.3.5 Mirror

ESET Mail Security consente all'utente di creare copie dei file di aggiornamento che è possibile utilizzare per aggiornare altre workstation della rete. Utilizzo di un *"mirror"*: è utile disporre di una copia dei file di aggiornamento nell'ambiente LAN, in quanto in questo modo i file di aggiornamento non devono essere scaricati ripetutamente dal server di aggiornamento del fornitore da ogni singola workstation. Gli aggiornamenti vengono scaricati sul server del mirror locale e distribuiti a tutte le workstation, allo scopo di evitare il rischio di un sovraccarico del traffico di rete. L'aggiornamento delle workstation client da un mirror consente di ottimizzare il bilanciamento del carico di rete e di risparmiare ampiezza di banda per la connessione a Internet.

Le opzioni di configurazione del server del mirror locale sono collocate in Configurazione avanzata sotto a **Aggiornamento**. Per accedere a questa sezione, premere F5; per accedere a Configurazione avanzata, fare clic su **Aggiornamento** e selezionare la scheda **Mirror**.

Per creare un mirror su una workstation client, attivare **Crea mirror di aggiornamento**. Attivando questa opzione, vengono attivate altre opzioni di configurazione del mirror, come la modalità di accesso ai file di aggiornamento e il percorso di aggiornamento per i file con mirroring.

Accesso ai file di aggiornamento

Fornisci i file di aggiornamento tramite il server HTTP interno: se questa opzione è attiva, è possibile accedere ai file di aggiornamento tramite HTTP senza che vengano richieste le credenziali.

NOTA: Windows XP richiede il Service Pack 2 o versioni successive per l'utilizzo del server HTTP.

I metodi per accedere al server del mirror sono descritti in dettaglio in Aggiornamento dal mirror. Sono disponibili due metodi di base per l'accesso al mirror: la cartella con i file di aggiornamento può essere presentata come cartella di rete condivisa oppure i client possono accedere al mirror collocato su un server HTTP.

La cartella dedicata alla memorizzazione dei file di aggiornamento per il mirror è definita sotto a **Cartella per l'archiviazione dei file con mirroring**. Fare clic su **Cartella** per cercare una cartella sul computer locale o una cartella di rete condivisa. Se è necessaria l'autorizzazione per la cartella specificata, i dati di autenticazione devono essere inseriti nei campi **Nome utente** e **Password**. Se la cartella di destinazione selezionata si trova su un disco di rete sul quale viene eseguito un sistema operativo Windows NT/2000/XP, il nome utente e la password specificati devono possedere i privilegi di scrittura per la cartella selezionata. Nome utente e password devono essere specificati nel formato *Dominio/Utente* o *Gruppodilavoro/Utente*. È necessario specificare le password corrispondenti.

File: durante la configurazione del mirror, è possibile specificare le lingue degli aggiornamenti che si desidera scaricare. Le lingue selezionate devono essere supportate dal server del mirror configurato dall'utente.

Server HTTP

Porta server: per impostazione predefinita, la porta del server è impostata su 2221.

Autenticazione: definisce il metodo di autenticazione utilizzato per l'accesso ai file di aggiornamento. Sono disponibili le seguenti opzioni: **Nessuno**, **Di base** e **NTLM**. Selezionare **Di base** per utilizzare la codifica base64 con l'autenticazione di base di nome utente e password. L'opzione **NTLM** offre una codifica basata sull'utilizzo di un metodo sicuro. Per l'autenticazione, viene utilizzato l'utente creato sulla workstation che condivide i file di aggiornamento. L'impostazione predefinita è **NESSUNO**, che garantisce l'accesso ai file di aggiornamento senza che sia necessaria l'autenticazione.

Se si desidera eseguire il server HTTP con il supporto HTTPS (SSL), è necessario aggiungere il **File della catena di certificato** o generare un certificato autofirmato. Sono disponibili i seguenti tipi di certificati: ASN, PEM e PFX. Per un livello di protezione aggiuntivo, è possibile utilizzare il protocollo HTTPS per scaricare i file di aggiornamento. Tramite questo protocollo, è quasi impossibile tenere traccia dei trasferimenti di dati e delle credenziali di accesso. Per impostazione predefinita, l'opzione **Tipo di chiave privata** è impostata su **Integrato** (e, di conseguenza, per impostazione predefinita, l'opzione **File della chiave privata** è disattivata). Ciò significa che la chiave privata fa parte del file della catena di certificati selezionato.

Connetti a LAN come

Tipo di utente locale: le impostazioni **Account di sistema (predefinito)**, **Utente corrente** e **Utente specificato** verranno visualizzate nei menu a discesa corrispondenti. Le impostazioni **Nome utente** e **Password** sono facoltative. Consultare Connetti a LAN come.

Selezionare **Disconnetti dal server dopo l'aggiornamento** per forzare una disconnessione se una connessione al server rimane attiva dopo il download degli aggiornamenti.

Aggiornamento dei componenti di programma

Aggiorna automaticamente i componenti: consente di eseguire l'installazione di nuove funzionalità e degli aggiornamenti di quelle esistenti. Un aggiornamento può essere eseguito automaticamente senza alcun intervento da parte dell'utente oppure è possibile scegliere di ricevere una notifica. Una volta installato l'aggiornamento dei componenti di programma, potrebbe essere necessario riavviare il computer.

Aggiorna componenti ora: installa l'ultima versione dei componenti del programma.

5.3.5.1 Aggiornamento dal mirror

Per configurare un mirror, che rappresenta essenzialmente un archivio in cui i client possono scaricare i file di aggiornamento, è possibile adottare due metodi di base. La cartella con i file di aggiornamento può essere presentata come cartella di rete condivisa o server HTTP.

Accesso al mirror mediante un server HTTP interno

Si tratta della configurazione predefinita specificata nell'impostazione originale del programma. Per consentire l'accesso al mirror tramite il server HTTP, accedere a **Configurazione avanzata** > **Aggiornamento** > **Mirror** e selezionare **Crea mirror di aggiornamento**.

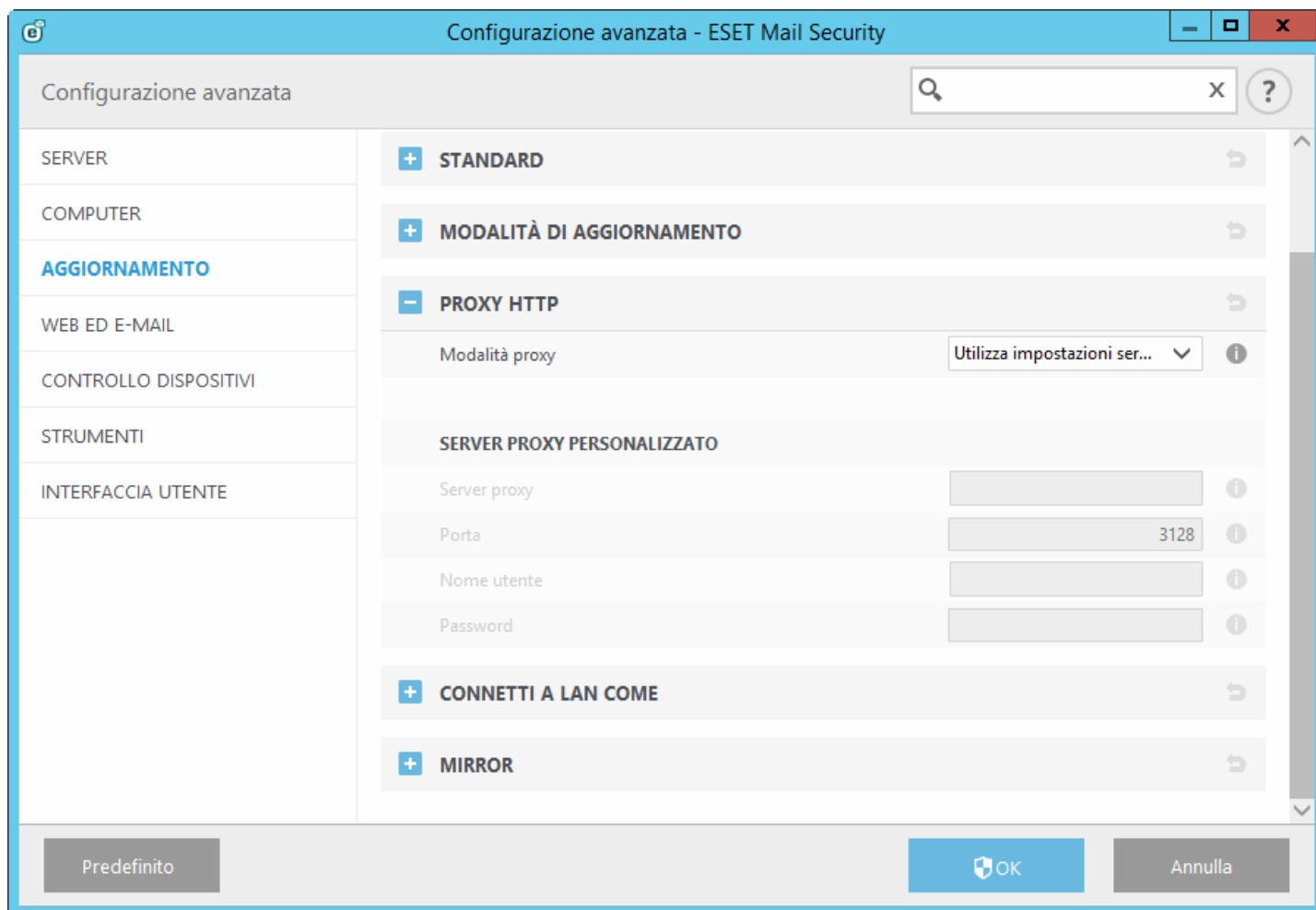
Nella sezione **Server HTTP** della scheda **Mirror**, è possibile specificare la **Porta server** di ascolto del server HTTP oltre al tipo di **Autenticazione** utilizzata dal server HTTP. Per impostazione predefinita, la porta del server è configurata su **2221**. L'opzione **Autenticazione** definisce il metodo di autenticazione utilizzato per l'accesso ai file di aggiornamento. Sono disponibili le seguenti opzioni: **Nessuno**, **Standard** e **NTLM**.

- Selezionare **Di base** per utilizzare la codifica base64 con l'autenticazione di base di nome utente e password.
- L'opzione **NTLM** offre una codifica basata sull'utilizzo di un metodo sicuro. Per l'autenticazione, viene utilizzato l'utente creato sulla workstation che condivide i file di aggiornamento.
- L'impostazione predefinita è **Nessuno**, che garantisce l'accesso ai file di aggiornamento senza che sia necessaria l'autenticazione.

Avviso: se si desidera consentire l'accesso ai file di aggiornamento tramite il server HTTP, la cartella Mirror deve essere posizionata sullo stesso computer dell'istanza di ESET Mail Security che la crea.

SSL per server HTTP

Se si desidera eseguire il server HTTP con il supporto HTTPS (SSL), è necessario aggiungere il **File della catena di certificato** o generare un certificato autofirmato. Sono disponibili i seguenti tipi di certificati: **PEM, PFX** e **ASN**. Per un livello di protezione aggiuntivo, è possibile utilizzare il protocollo HTTPS per scaricare i file di aggiornamento. Tramite questo protocollo, è quasi impossibile tenere traccia dei trasferimenti di dati e delle credenziali di accesso. L'opzione **Tipo di chiave privata** è impostata su **Integrata** per impostazione predefinita e ciò significa che la chiave privata fa parte del file della catena di certificati selezionato.

i **NOTA**: nel riquadro Aggiornamento del menu principale comparirà l'errore **Nome utente e/o password non validi** dopo vari tentativi non riusciti di aggiornamento del database delle firme antivirali dal mirror. Si consiglia di accedere a **Configurazione avanzata** > **Aggiornamento**> **Mirror** e controllare il nome utente e la password. Il motivo più comune alla base di questo errore consiste in un inserimento errato dei dati di autenticazione.

Dopo aver configurato il server mirror, è necessario aggiungere il nuovo server di aggiornamento sulle workstation client. Per eseguire questa operazione, effettuare i seguenti passaggi:

- Accedere a **Configurazione avanzata** (F5) e fare clic su **Aggiornamento** > **Di base**.
- Disattivare **Scegli automaticamente** e aggiungere un nuovo server nel campo **Server di aggiornamento** utilizzando uno dei seguenti formati:
  http://indirizzo_IP_del_server:2221
  https://indirizzo_IP_del_server_in_uso:2221 (in caso di utilizzo di SSL)

Accesso al mirror tramite le condivisioni di sistema

È innanzitutto necessario creare una cartella condivisa su un dispositivo locale o di rete. Durante la creazione della cartella per il mirror, è necessario garantire l'accesso *"in scrittura"* all'utente che salverà i file di aggiornamento nella cartella e l'accesso *"in lettura"* a tutti gli utenti che aggiorneranno ESET Mail Security dalla cartella Mirror.

Configurare quindi l'accesso al mirror nella scheda **Configurazione avanzata** > **Aggiornamento** > **Mirror** disattivando **Fornisci i file di aggiornamento tramite il server HTTP interno**. Questa opzione è attivata per impostazione predefinita nel pacchetto di installazione del programma.

Se la cartella condivisa è posizionata su un altro computer della rete, sarà necessario immettere i dati di autenticazione per l'accesso all'altro computer. Per immettere i dati di autenticazione, aprire **Configurazione avanzata di** ESET Mail Security (F5) e fare clic su **Aggiornamento** > **Connetti a LAN come**. Questa è la stessa impostazione utilizzata per l'aggiornamento, come illustrato nella sezione Connetti a LAN come.

Una volta completata la configurazione del mirror, sulle workstation client impostare *\\UNC\PERCORSO* come server di aggiornamento seguendo la procedura sottostante:

1. Aprire Configurazione avanzata di ESET Mail Security e fare clic su **Aggiornamento** > **Di base**.
2. Fare clic su **Server di aggiornamento** e aggiungere un nuovo server utilizzando il formato *\\UNC\PERCORSO*.

NOTA: per un corretto funzionamento degli aggiornamenti, il percorso alla cartella Mirror deve essere specificato come percorso UNC. Gli aggiornamenti provenienti dalle unità mappate potrebbero non funzionare.

L'ultima sezione controlla i componenti di programma (PCU). Per impostazione predefinita, i componenti di programma scaricati vengono preparati per la copia sul mirror locale. Se **Aggiornamento dei componenti di programma** è attivo, non è necessario fare clic su **Aggiorna**, in quanto i file vengono copiati automaticamente sul mirror locale nel momento in cui sono disponibili. Per ulteriori informazioni sugli aggiornamenti dei componenti di programma, consultare Modalità di aggiornamento.

5.3.5.2 File mirror

Elenco dei file dei componenti del programma disponibili e localizzati.

5.3.5.3 Risoluzione dei problemi di aggiornamento del mirror

Nella maggior parte dei casi, i problemi durante un aggiornamento da un server mirror sono causati da uno o più motivi, tra cui: specifica non corretta delle opzioni della cartella Mirror, autenticazione non corretta dei dati per la cartella Mirror, configurazione non corretta sulle workstation locali che tentano di scaricare i file di aggiornamento dal mirror o una combinazione di questi motivi. Di seguito viene riportata una panoramica dei problemi più frequenti che potrebbero verificarsi durante un aggiornamento eseguito dal mirror:

- **ESET Mail Security riporta un errore di connessione al server mirror**: probabilmente causato da una specifica non corretta del server di aggiornamento (percorso di rete alla cartella Mirror) dal quale le workstation locali scaricano gli aggiornamenti. Per verificare la cartella, selezionare il menu **Start** di Windows, fare clic su **Esegui**, immettere il nome della cartella e selezionare **OK**. Dovrebbe essere visualizzato il contenuto della cartella.
- **ESET Mail Security richiede un nome utente e una password**: probabilmente causato dall'immissione di dati di autenticazione (nome utente e password) non corretti nella sezione di aggiornamento. Il nome utente e la password sono utilizzati per concedere l'accesso al server di aggiornamento dal quale il programma si aggiornerà. Verificare che i dati di autenticazione siano corretti e immessi nel formato appropriato. Ad esempio, *Dominio/Nome utente* o *Gruppo di lavoro/Nome utente*, oltre alle password corrispondenti. Se il server mirror è accessibile a "Tutti", tenere presente che ciò non significa che l'accesso è concesso a qualsiasi utente. Con "Tutti" non si intendono tutti gli utenti non autorizzati. Si intende solo che la cartella è accessibile a tutti gli utenti del dominio. Di conseguenza, se una cartella è accessibile a "Tutti", sarà comunque necessario specificare un nome utente di dominio e una password nella sezione di configurazione dell'aggiornamento.
- **ESET Mail Security riporta un errore di connessione al server mirror**: la comunicazione sulla porta definita per l'accesso alla versione HTTP del mirror è bloccata.

5.3.6 Come fare per creare attività di aggiornamento

È possibile avviare gli aggiornamenti manualmente selezionando l'opzione **Aggiorna database delle firme antivirali** nella finestra principale visualizzata dopo aver selezionato l'opzione **Aggiorna** dal menu principale.

Gli aggiornamenti possono essere eseguiti anche come attività programmate. Per configurare un'attività programmata, fare clic su **Strumenti** > **Pianificazione attività**. Per impostazione predefinita, in ESET Mail Security sono attivate le seguenti attività:

- **Aggiornamento automatico periodico**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**

È possibile modificare ciascuna delle attività di aggiornamento in base alle proprie esigenze. Oltre alle attività di aggiornamento predefinite, è possibile creare nuove attività di aggiornamento con una configurazione definita dall'utente. Per ulteriori dettagli sulla creazione e sulla configurazione delle attività di aggiornamento, consultare la sezione Pianificazione attività di questa guida.

5.4 Web e e-mail

La sezione **Web e e-mail** consente di configurare la Protezione client di posta, proteggere la comunicazione su Internet mediante la Protezione accesso Web e controllare i protocolli Internet configurando il Filtraggio protocolli. Queste funzionalità sono essenziali per proteggere il computer durante le comunicazioni effettuate tramite Internet.

La **Protezione client di posta** controlla tutte le comunicazioni e-mail, protegge da codici dannosi e consente all'utente di scegliere l'azione da eseguire quando viene rilevata un'infezione.

La **Protezione accesso Web** monitora la comunicazione tra i browser Web e i server remoti ed è conforme alle regole HTTP e HTTPS. Questa funzionalità consente inoltre di bloccare, consentire o escludere alcuni Indirizzi URL.

Il **Filtraggio protocolli** è una protezione avanzata per i protocolli delle applicazioni che viene fornita dal motore di controllo ThreatSense. Questo controllo funziona automaticamente, indipendentemente dal browser Web o dal client di posta in uso. Funziona anche per la comunicazione crittografata (SSL).

5.4.1 Filtraggio protocolli

Filtraggio protocolli

La protezione antivirus per i protocolli delle applicazioni viene offerta dal motore di controllo ThreatSense, che integra perfettamente tutte le tecniche di controllo avanzato dei malware. Il filtraggio protocolli funziona automaticamente, indipendentemente dal browser Internet o dal client di posta in uso. Per modificare le impostazioni crittografate (SSL), accedere a **Web e e-mail** > **Controllo protocollo SSL**.

Attiva filtraggio contenuto protocollo applicazioni: può essere utilizzato per disattivare il filtraggio dei protocolli. Tenere presente che il funzionamento di numerosi componenti di ESET Mail Security (protezione accesso Web, protezione protocolli e-mail e Anti-Phishing) dipende interamente da questa funzione.

Applicazioni escluse: consente all'utente di escludere indirizzi remoti specifici dal filtraggio protocolli. Questa funzione è utile in caso di problemi di compatibilità causati dal filtraggio protocolli.

Indirizzi IP esclusi: consente all'utente di escludere applicazioni specifiche dal filtraggio protocolli. Questa funzione è utile in caso di problemi di compatibilità causati dal filtraggio protocolli.

Client Web e di posta: questa funzione, utilizzata solo sui sistemi operativi Windows, consente all'utente di selezionare le applicazioni per cui l'intero traffico viene filtrato dal filtraggio protocolli, indipendentemente dalle porte utilizzate.

Registra le informazioni necessarie al supporto ESET per diagnosticare i problemi correlati al filtraggio dei protocolli: attiva la registrazione avanzata dei dati diagnostici; utilizzare questa funzione solo se richiesto dal supporto ESET.

5.4.1.1 Applicazioni escluse

Per escludere la comunicazione di specifiche applicazioni di rete dal filtraggio dei contenuti, selezionarle nell'elenco. Sulla comunicazione HTTP/POP3 delle applicazioni selezionate non verrà eseguito il rilevamento delle minacce. È consigliabile usare questa opzione solo per le applicazioni che non funzionano correttamente se la rispettiva comunicazione viene sottoposta a controllo.

Le applicazioni e i servizi sui quali è già stato attivato il filtraggio protocolli verranno visualizzati automaticamente facendo clic su **Aggiungi**.

Modifica: modifica le voci selezionate dall'elenco.

Rimuovi: rimuove dall'elenco le voci selezionate.

5.4.1.2 Indirizzi IP esclusi

Gli indirizzi IP presenti in questo elenco verranno esclusi dal filtraggio dei contenuti del protocollo. Sulla comunicazione HTTP/POP3/IMAP da/verso gli indirizzi selezionati non verrà eseguito il rilevamento delle minacce. È consigliabile utilizzare questa opzione solo per gli indirizzi di cui è nota l'affidabilità.

Aggiungi: fare clic per aggiungere un indirizzo IP/intervallo di indirizzi/subnet di un punto remoto a cui viene applicata una regola.

Modifica: modifica le voci selezionate dall'elenco.

Rimuovi: rimuove dall'elenco le voci selezionate.

5.4.1.3 Web e client di posta

i **NOTA:** in Windows Vista Service Pack 1 e Windows Server 2008 per il controllo delle comunicazioni di rete viene utilizzata la nuova architettura Windows Filtering Platform (WFP). Poiché la tecnologia WPF utilizza speciali tecniche di monitoraggio, la sezione **Web e client di posta** non è disponibile.

A causa dell'enorme quantità di codice dannoso che circola su Internet, una navigazione Internet sicura è essenziale per la protezione del computer. Le vulnerabilità dei browser Web e i collegamenti fraudolenti aiutano il codice dannoso a penetrare inosservato nel sistema. Per tale motivo, ESET Mail Security si focalizza sulla sicurezza dei browser Web. Ogni applicazione che accede alla rete può essere contrassegnata come un browser. Nell'elenco di client Web e di posta, è possibile aggiungere le applicazioni che utilizzano già protocolli di comunicazione o applicazioni provenienti dai percorsi selezionati.

5.4.2 Verifica protocollo SSL

ESET Mail Security è in grado di ricercare le minacce contenute nelle comunicazioni che utilizzano il protocollo SSL. È possibile utilizzare varie modalità di controllo per l'analisi delle comunicazioni protette dal protocollo SSL con certificati attendibili, certificati sconosciuti o certificati che sono esclusi dal controllo delle comunicazioni protette dal protocollo SSL.

Attiva filtraggio protocollo SSL: se il filtraggio protocolli è disattivato, il programma non controllerà le comunicazioni sull'SSL.

La **Modalità filtraggio protocollo SSL** è disponibile nelle seguenti opzioni:

- **Modalità automatica**: selezionare questa opzione per controllare tutte le comunicazioni protette dal protocollo SSL ad eccezione delle comunicazioni protette dai certificati esclusi dal controllo. Se viene stabilita una nuova comunicazione utilizzando un certificato firmato sconosciuto, all'utente non verrà inviata alcuna notifica e la comunicazione verrà filtrata in modo automatico. Quando si accede a un server con un certificato non attendibile contrassegnato come attendibile (presente nell'elenco dei certificati attendibili), la comunicazione con il server è consentita e il contenuto del canale di comunicazione viene filtrato.

- **Modalità interattiva**: all'accesso a un nuovo sito protetto da SSL (con un certificato sconosciuto), viene visualizzata una finestra di dialogo per la scelta dell'azione. Questa modalità consente di creare un elenco di certificati SSL che verranno esclusi dal controllo.

Blocca le comunicazioni crittografate che utilizzano il protocollo obsoleto SSL v2: la comunicazione che utilizza la versione precedente del protocollo SSL verrà automaticamente bloccata.

Certificato radice

Certificato radice: affinché la comunicazione SSL funzioni in modo adeguato nei browser/client di posta dell'utente, è fondamentale che il certificato radice di ESET venga aggiunto all'elenco dei certificati radice noti (autori). È necessario attivare **Aggiungi il certificato radice ai browser conosciuti**. Selezionare questa opzione per aggiungere automaticamente il certificato radice di ESET ai browser conosciuti (ad esempio, Opera e Firefox). Per i browser che utilizzano l'archivio di certificazioni di sistema, il certificato viene aggiunto automaticamente (ad esempio, Internet Explorer).

Per applicare il certificato a browser non supportati, fare clic su **Visualizza certificato** > **Dettagli** > **Copia su file...** e importarlo manualmente nel browser.

Validità del certificato

Se il certificato non può essere verificato mediante l'utilizzo dell'archivio certificati TRCA: in alcuni casi, non è possibile verificare la validità del certificato di un sito Web utilizzando l'archivio Autorità di certificazione radice attendibili (TRCA). Ciò significa che il certificato è firmato da qualcuno (ad esempio, l'amministratore di un server Web o una piccola azienda) e considerare questo certificato come attendibile non rappresenta sempre un rischio per la sicurezza. Gran parte delle aziende di maggior dimensioni (ad esempio, le banche) utilizza un certificato firmato dal TRCA. Dopo aver selezionato **Chiedi conferma della validità dei certificati** (impostazione predefinita), all'utente verrà richiesto di selezionare un'azione da eseguire in caso di comunicazione crittografata. È possibile selezionare **Blocca comunicazioni che utilizzano il certificato** per terminare sempre le connessioni crittografate ai siti con certificati non verificati.

Se il certificato è danneggiato o non valido: ciò significa che il certificato è scaduto o che la firma era errata. In questo caso, è consigliabile lasciare selezionata l'opzione **Blocca comunicazioni che utilizzano il certificato**.

L'**Elenco di certificati noti** consente all'utente di personalizzare il comportamento di ESET Mail Security per specifici certificati SSL.

5.4.2.1 Comunicazioni SSL crittografate

Se il sistema in uso è configurato in modo da utilizzare il controllo del protocollo SSL, in due situazioni verrà visualizzata una finestra di dialogo che richiede all'utente di scegliere un'azione:

Innanzitutto, se un sito Web utilizza un certificato non verificabile o non valido e ESET Mail Security è configurato in modo da chiedere la conferma dell'utente in tali casi (per impostazione predefinita, sì per i certificati non verificabili e no per quelli non validi), una finestra di dialogo chiederà all'utente di **Consentire** o **Bloccare** la connessione.

In secondo luogo, se la **Modalità filtraggio protocollo SSL** è impostata su **Modalità interattiva**, una finestra di dialogo per ciascun sito Web chiederà all'utente di **Controllare** o **Ignorare** il traffico. Alcune applicazioni verificano che il relativo traffico SSL non sia né modificato né ispezionato da terzi e, in casi come questo, ESET Mail Security deve **Ignorare** il traffico per consentire all'applicazione di continuare a funzionare.

In entrambi i casi, l'utente può scegliere di ricordare l'azione selezionata. Le azioni salvate vengono archiviate nell'**Elenco di certificati noti**.

5.4.2.2 Elenco di certificati noti

L'elenco di certificati noti può essere utilizzato per la personalizzazione del comportamento di ESET Mail Security per specifici certificati SSL e per ricordare le azioni scelte qualora, in Modalità filtraggio protocollo SSL, venga selezionata la modalità interattiva. L'elenco può essere visualizzato e modificato in **Configurazione avanzata** (F5) > **Web e e-mail** > **Controllo protocollo SSL** > **Elenco di certificati noti**.

La finestra **Elenco di certificati noti** è formata da:

Colonne

- **Nome** : nome del certificato.
- **Autorità di certificazione emittente**: nome del creatore del certificato.
- **Oggetto certificato**: campo dell'oggetto che identifica l'entità associata alla chiave pubblica archiviata nel campo Chiave pubblica dell'oggetto.
- **Accesso:** selezionare **Consenti** o **Blocca** come **Azione di accesso** per consentire/bloccare la comunicazione protetta da questo certificato indipendentemente dalla sua attendibilità. Selezionare **Auto** per consentire i certificati attendibili e richiedere quelli inattendibili. Selezionare **Chiedi** per chiedere sempre all'utente cosa fare.
- **Controlla**: selezionare**Controlla** o **Ignora** come **Azione di controllo** per controllare o ignorare la comunicazione protetta da questo certificato. Selezionare **Auto** per eseguire il controllo in modalità automatica e attivare la richiesta in modalità interattiva. Selezionare **Chiedi** per chiedere sempre all'utente cosa fare.

Elementi di controllo

- **Modifica**: selezionare il certificato che si desidera configurare e fare clic su **Modifica**.
- **Rimuovi**: selezionare il certificato che si desidera eliminare e fare clic su **Rimuovi**.
- **OK/Annulla**: fare clic su **OK** se si desidera salvare le modifiche o su **Annulla** se si desidera uscire senza salvare.

5.4.3 Protezione client di posta

L'integrazione di ESET Mail Security con i client di posta aumenta il livello di protezione attiva contro codici dannosi nei messaggi di posta elettronica. Se il client di posta in uso è supportato, è possibile attivare l'integrazione in ESET Mail Security. In caso di attivazione dell'integrazione, la barra degli strumenti di ESET Mail Security viene inserita direttamente nel client di posta (ad eccezione di quella relativa alle versioni più recenti di Windows Live Mail), garantendo in tal modo una protezione più efficiente delle e-mail. Le impostazioni relative all'integrazione sono collocate sotto a **Configurazione** > **Configurazione avanzata** > **Web e e-mail** > **Protezione client di posta** > **Client di posta**.

Integrazione client di posta

I client di posta attualmente supportati sono Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. Per questi programmi, la protezione e-mail funziona come un plug-in. Il vantaggio principale offerto dal plug-in consiste nella sua indipendenza dal protocollo utilizzato. Quando il client di posta riceve un messaggio crittografato, questo viene decodificato e inviato allo scanner antivirus. Per un elenco completo dei client di posta supportati e delle relative versioni, consultare il seguente articolo della Knowledge Base ESET.

Anche se l'integrazione non è attivata, la comunicazione e-mail rimane comunque protetta tramite il modulo di protezione client di posta (POP3, IMAP).

Attivare **Disattiva il controllo alla modifica del contenuto della posta in arrivo** se si riscontra un rallentamento del sistema durante l'utilizzo del client di posta (solo MS Outlook). Ciò può accadere durante il recupero di e-mail da Kerio Outlook Connector Store.

E-mail da controllare

E-mail ricevuta: attiva/disattiva il controllo dei messaggi ricevuti.
E-mail inviata: attiva/disattiva il controllo dei messaggi inviati.
E-mail letta: attiva/disattiva il controllo dei messaggi letti.

Azione da eseguire sull'e-mail infetta

Nessuna azione: se questa opzione è attivata, il programma identificherà gli allegati infetti senza tuttavia eseguire alcuna azione.
Elimina e-mail: il programma notificherà all'utente l'eventuale o le eventuali infiltrazioni ed eliminerà il messaggio.
Sposta e-mail nella cartella Posta eliminata: le e-mail infette verranno spostate automaticamente nella cartella Posta eliminata.
Sposta e-mail nella cartella: le e-mail infette verranno spostate automaticamente nella cartella specificata.

Cartella: specificare la cartella personalizzata in cui si desidera spostare le e-mail infette una volta rilevate.

Ripeti controllo dopo l'aggiornamento: attiva/disattiva un nuovo controllo dopo l'aggiornamento del database delle firme antivirali.

Accetta i risultati del controllo da altri moduli: selezionando questa opzione, il modulo di protezione e-mail accetterà i risultati del controllo eseguito da altri moduli di protezione (controllo protocolli POP3, IMAP).

5.4.3.1 Protocolli e-mail

IMAP e POP3 sono i protocolli più comunemente utilizzati per ricevere comunicazioni e-mail in un'applicazione client di posta. ESET Mail Security offre protezione per questi protocolli indipendentemente dal client di posta utilizzato e senza richiederne la riconfigurazione.

È possibile configurare il controllo dei protocolli IMAP/IMAPS e POP3/POP3S in Configurazione avanzata. Per accedere a questa impostazione, espandere **Web e e-mail** > **Protezione client di posta** > **Protocolli e-mail**.

ESET Mail Security supporta anche il controllo dei protocolli IMAPS e POP3S che utilizzano un canale crittografato per trasferire le informazioni tra il server e il client. ESET Mail Security controlla la comunicazione utilizzando i protocolli SSL (Secure Socket Layer) e TLS (Transport Layer Security). Il programma controllerà esclusivamente il traffico sulle porte definite in Porte utilizzate dal protocollo HTTPS/POP3S, indipendentemente dalla versione del sistema operativo.

Le comunicazioni crittografate non verranno controllate durante l'utilizzo delle impostazioni predefinite. Per attivare il controllo della comunicazione crittografata, accedere a Verifica protocollo SSL in Configurazione avanzata, fare clic su **Web e e-mail** > **Verifica protocollo SSL** e selezionare **Attiva filtraggio protocollo SSL**.

5.4.3.2 Avvisi e notifiche

La Protezione client di posta garantisce il controllo delle comunicazioni e-mail ricevute mediante i protocolli POP3 e IMAP. Utilizzando il plug-in per Microsoft Outlook e altri client di posta, ESET Mail Security controlla tutte le comunicazioni dal client di posta (POP3, MAPI, IMAP, HTTP). Durante la verifica dei messaggi in arrivo, il programma utilizza tutti i metodi di controllo avanzato previsti nel motore di controllo ThreatSense. Ciò significa che il rilevamento di programmi dannosi viene eseguito ancora prima del confronto con il database delle firme antivirali. Il controllo delle comunicazioni mediante i protocolli POP3 e IMAP non dipende dal client di posta in uso.

Le opzioni di questa funzionalità sono disponibili in **Configurazione avanzata** sotto a **Web e e-mail** > **Protezione client di posta** > **Avvisi e notifiche**.

Parametri ThreatSense: la configurazione avanzata dello scanner antivirus consente all'utente di configurare le destinazioni di controllo, i metodi di rilevamento e così via. Fare clic per visualizzare la finestra della configurazione dettagliata dello scanner antivirus.

Dopo che un messaggio e-mail è stato controllato, è possibile aggiungere una notifica contenente i risultati del controllo. È possibile scegliere le opzioni **Aggiungi notifiche all'e-mail ricevuta e letta, Aggiungi nota all'oggetto dell'e-mail infetta ricevuta e letta** o l'opzione **Aggiungi notifiche all'e-mail inviata**. Tenere presente che, in rare occasioni, le notifiche potrebbero essere omesse in messaggi HTML problematici o creati da malware. Le notifiche possono essere aggiunte sia alle e-mail ricevute e lette sia alle e-mail inviate. Le opzioni disponibili sono:

- **Mai**: non viene aggiunta alcuna notifica.
- **Solo per l'e-mail infetta**: solo i messaggi contenenti software dannoso vengono contrassegnati come controllati (impostazione predefinita).
- **Per tutte le e-mail** : il programma aggiunge la notifica a tutte le e-mail sottoposte a controllo.

Aggiungi nota all'oggetto dell'e-mail infetta inviata: disattivare questa opzione se non si desidera che la protezione e-mail includa un avviso antivirus nell'oggetto di un'e-mail infetta. Questa funzione consente di filtrare in modo semplice le e-mail infette in base all'oggetto (se supportata dal programma e-mail in uso). Aumenta inoltre il livello di credibilità del destinatario e, in caso di rilevamento di un'infiltrazione, fornisce informazioni utili sul livello di minaccia di un determinato messaggio e-mail o mittente.

Modello aggiunto all'oggetto dell'e-mail infetta: modificare questo template se si desidera cambiare il formato predefinito dell'oggetto di un'e-mail infetta. Questa funzione sostituirà l'oggetto del messaggio *"Ciao"* con un determinato valore predefinito *"[virus]"* nel seguente formato: *"[virus] Ciao"*. La variabile *%VIRUSNAME%* rappresenta la minaccia rilevata.

5.4.3.3 Barra degli strumenti di MS Outlook

La protezione di Microsoft Outlook ha la stessa funzione di un modulo plug-in. Dopo aver installato ESET Mail Security, la barra degli strumenti contenente le opzioni della protezione antivirus verrà aggiunta a Microsoft Outlook:

ESET Mail Security: fare clic sull'icona per aprire la finestra principale del programma ESET Mail Security.

Ripeti controllo messaggi: consente di avviare manualmente il controllo e-mail. È possibile specificare i messaggi da controllare e attivare un nuovo controllo dei messaggi e-mail ricevuti. Per ulteriori informazioni, consultare Protezione client di posta.

Configurazione scanner: consente di visualizzare le opzioni per la configurazione della Protezione client di posta.

5.4.3.4 Barra degli strumenti di Outlook Express e Windows Mail

La protezione per Outlook Express e Windows Mail funziona come un modulo plug-in. Dopo aver installato ESET Mail Security, la barra degli strumenti contenente le opzioni della protezione antivirus verrà aggiunta a Outlook Express o Windows Mail:

ESET Mail Security: fare clic sull'icona per aprire la finestra principale del programma ESET Mail Security.

Ripeti controllo messaggi: consente di avviare manualmente il controllo e-mail. È possibile specificare i messaggi da controllare e attivare un nuovo controllo dei messaggi e-mail ricevuti. Per ulteriori informazioni, consultare Protezione client di posta.

Configurazione scanner: consente di visualizzare le opzioni per la configurazione della Protezione client di posta.

Interfaccia utente

Personalizza aspetto: è possibile modificare l'aspetto della barra degli strumenti del client di posta. Deselezionare l'opzione per personalizzare l'aspetto indipendentemente dai parametri del client di posta.

Visualizza testo: consente di visualizzare la descrizione delle operazioni rappresentate dalle icone.

Testo a destra: la descrizione delle opzioni viene spostata a destra delle icone.

Icone grandi: consente di visualizzare icone grandi per le opzioni di menu.

5.4.3.5 Finestra di dialogo di conferma

Questo messaggio di notifica serve a verificare che l'utente intenda davvero effettuare l'azione selezionata, evitando in questo modo possibili errori.

In questa finestra di dialogo è anche possibile disattivare le richieste di conferma tramite l'apposita opzione.

5.4.3.6 Ripeti controllo messaggi

La barra degli strumenti di ESET Mail Security integrata nei client di posta consente agli utenti di indicare diverse opzioni di controllo e-mail. L'opzione **Ripeti controllo messaggi** offre due modalità di controllo:

Tutti i messaggi nella cartella corrente: esegue il controllo dei messaggi nella cartella visualizzata al momento.

Solo messaggi selezionati: esegue il controllo dei soli messaggi contrassegnati dall'utente.

La casella di controllo **Ripeti controllo sui messaggi già controllati** consente all'utente di eseguire un altro controllo sui messaggi che sono stati già controllati.

5.4.4 Protezione accesso Web

La connettività Internet è una funzione standard nella maggior parte dei personal computer. Purtroppo è diventato anche lo strumento principale per il trasferimento di codice dannoso. La Protezione accesso Web monitora la comunicazione tra i browser Web e i server remoti ed è conforme alle regole HTTP (Hypertext Transfer Protocol) e HTTPS (comunicazione crittografata).

L'accesso a pagine Web note per essere dannose è bloccato prima del download dei relativi contenuti. Tutte le altre pagine Web vengono controllate dal motore di controllo ThreatSense nel momento in cui vengono caricate e bloccate in caso di rilevamento di contenuti dannosi. La protezione accesso Web offre due livelli di protezione: il blocco in base alla blacklist e il blocco in base ai contenuti.

Si consiglia vivamente di lasciare l'opzione Protezione accesso Web attivata. L'opzione è disponibile dalla finestra principale del programma di ESET Mail Security accedendo a **Configurazione** > **Web e e-mail** > **Protezione accesso Web**.

Le seguenti opzioni sono disponibili in **Configurazione avanzata** (F5) > **Web e e-mail** > **Protezione accesso Web**:

- **Protocolli Web**: consente all'utente di configurare il monitoraggio di questi protocolli standard utilizzati dalla maggior parte dei browser Internet.
- **Gestione indirizzi URL**: consente all'utente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo.
- **Configurazione parametri motore ThreatSense**: configurazione avanzata scanner antivirus: consente all'utente di configurare impostazioni quali i tipi di oggetti da controllare (e-mail, archivi e così via.), i metodi di rilevamento della protezione accesso Web, ecc.

5.4.4.1 Gestione indirizzi URL

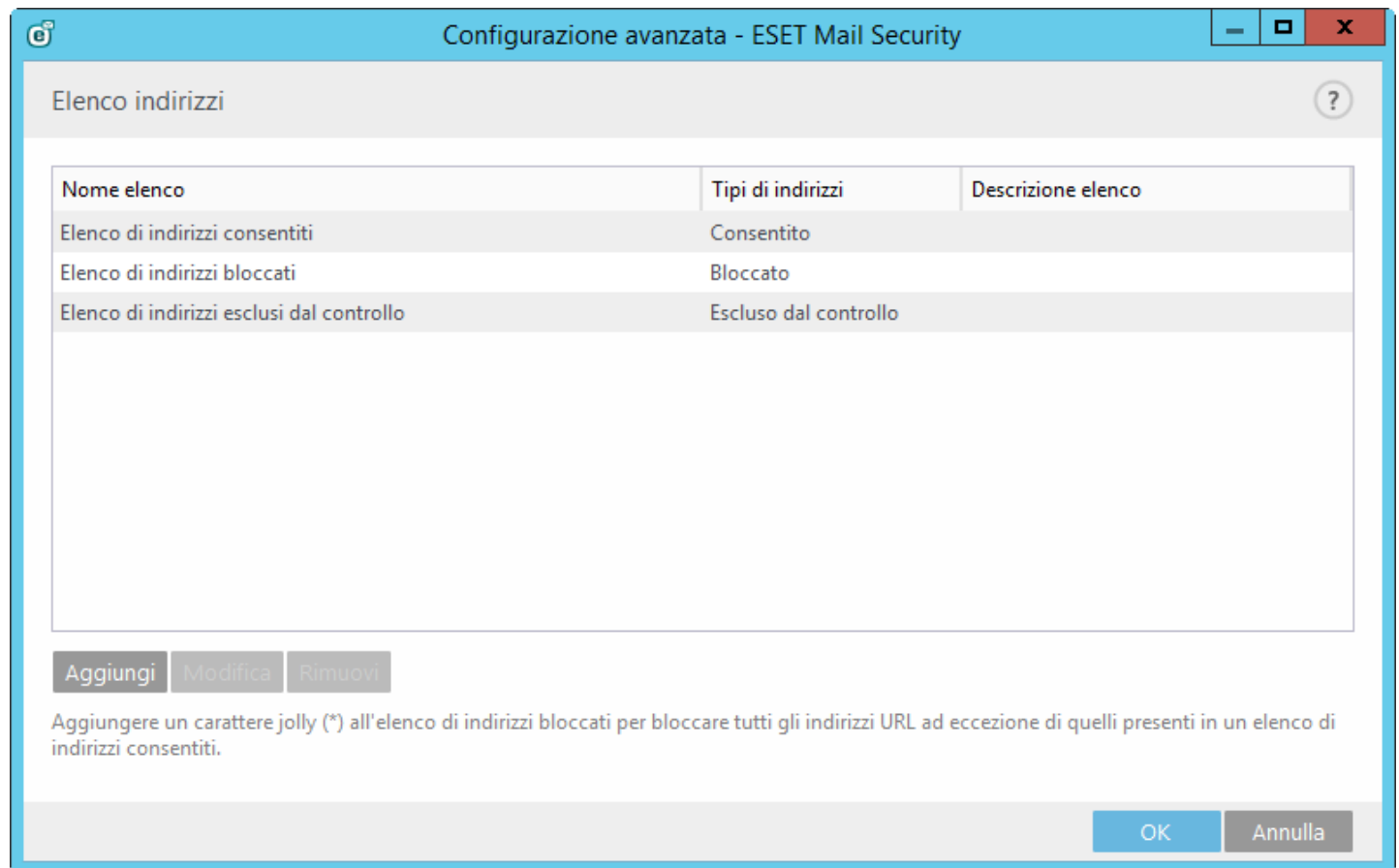
La sezione Gestione indirizzi URL consente all'utente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo.

I siti Web presenti nell'elenco di indirizzi bloccati non saranno accessibili a meno che non vengano inclusi nell'elenco di indirizzi consentiti. Nei siti Web presenti nell'elenco di indirizzi esclusi dal controllo non vengono ricercati codici dannosi al momento dell'accesso.

Se si desidera filtrare gli indirizzi HTTPS oltre alle pagine Web HTTP, è necessario selezionare **Attiva filtraggio protocollo SSL**. In caso contrario, verranno aggiunti solo i domini dei siti HTTPS visitati e non l'intero indirizzo URL.

In tutti gli elenchi è possibile utilizzare i simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco rappresenta un qualsiasi numero o carattere, mentre il punto interrogativo rappresenta un qualsiasi carattere. Prestare particolare attenzione quando si specificano gli indirizzi esclusi dal controllo, in quanto l'elenco deve contenere solo indirizzi attendibili e sicuri. Allo stesso modo, è necessario verificare che in questo elenco i simboli *

e ? siano utilizzati correttamente.

Se si desidera bloccare tutti gli indirizzi HTTP ad eccezione di quelli presenti nell'**Elenco di indirizzi consentiti** attivo, è necessario aggiungere * all'**Elenco di indirizzi bloccati** attivo.

Aggiungi: crea un nuovo elenco oltre a quelli predefiniti. Questa opzione è utile se si desidera suddividere vari gruppi di indirizzi in base a criteri logici. Ad esempio, un elenco di indirizzi bloccati potrebbe contenere indirizzi provenienti da blacklist pubbliche esterne e un altro la blacklist dell'utente. In tal modo, si facilita l'aggiornamento dell'elenco esterno mantenendo nel contempo intatto quello dell'utente.
Modifica: modifica gli elenchi esistenti. Utilizzare questa funzione per aggiungere o rimuovere indirizzi dagli elenchi.
Rimuovi: rimuove l'elenco esistente. Questa funzione è disponibile esclusivamente per gli elenchi creati con Aggiungi e non per quelli predefiniti.

5.4.4.1.1 Crea nuovo elenco

Questa sezione consente all'utente di specificare elenchi di indirizzi URL/maschere che verranno bloccati, consentiti o esclusi dal controllo.

Quando si crea un nuovo elenco, è possibile configurare le seguenti opzioni:

Tipo di elenco degli indirizzi: sono disponibili tre tipi di elenchi:

- **Elenco indirizzi esclusi dal controllo**: per gli indirizzi aggiunti a questo elenco non verrà eseguita la ricerca di codice dannoso.
- **Elenco di indirizzi bloccati**: all'utente non sarà consentito accedere agli indirizzi indicati in questo elenco. Ciò vale solo per il protocollo HTTP. I protocolli diversi dall'HTTP non verranno bloccati.
- **Elenco di indirizzi consentiti**: se l'opzione Consenti accesso solo agli indirizzi HTTP dell'elenco indirizzi consentiti è attiva e l'elenco di indirizzi bloccati contiene * (ricerca tutto), l'utente potrà accedere solo agli indirizzi specificati in questo elenco. Gli indirizzi in questo elenco sono consentiti anche se corrispondono anche a quelli inclusi nell'elenco di indirizzi bloccati.

Nome elenco: specificare il nome dell'elenco. Il campo verrà disattivato durante la modifica di uno dei tre elenchi predefiniti.

Descrizione elenco: digitare una breve descrizione per l'elenco (facoltativo). Verrà disattivato durante la modifica di uno dei tre elenchi predefiniti.

Per attivare un elenco, selezionare l'opzione **Elenco attivo** posizionata accanto. Se, in caso di utilizzo di un elenco specifico, si desidera ricevere una notifica contenente la valutazione di un sito HTTP visitato, selezionare **Notifica in caso di applicazione**. Ad esempio, verrà inviata una notifica se un sito Web viene bloccato o consentito perché incluso in un elenco di indirizzi rispettivamente bloccati o consentiti. La notifica conterrà il nome dell'elenco che include il sito Web specifico.

Aggiungi: aggiunge un nuovo indirizzo URL all'elenco (inserire valori multipli con separatore).

Modifica: modifica l'indirizzo esistente nell'elenco. Questa funzione è disponibile esclusivamente per gli indirizzi creati con Aggiungi.

Rimuovi: elimina gli indirizzi esistenti nell'elenco. Questa funzione è disponibile esclusivamente per gli indirizzi creati con Aggiungi.

Importa: importa un file con gli indirizzi URL (separare i valori con un'interruzione di riga, ad esempio *.txt, utilizzando la codifica UTF-8).

5.4.4.1.2 Indirizzi HTTP

In questa sezione, è possibile specificare elenchi di indirizzi HTTP che verranno bloccati, consentiti o esclusi dal controllo.

Per impostazione predefinita, sono disponibili i tre elenchi riportati di seguito:

- **Elenco indirizzi esclusi dal controllo**: per gli indirizzi aggiunti a questo elenco non verrà eseguita la ricerca di codice dannoso.
- **Elenco di indirizzi consentiti**: se **è attivato Consenti accesso solo agli indirizzi HTTP dell'elenco indirizzi consentiti** e l'elenco di indirizzi bloccati contiene * (ricerca tutto), l'utente potrà accedere solo agli indirizzi specificati in questo elenco. Gli indirizzi in questo elenco sono consentiti anche se inclusi nell'elenco di indirizzi bloccati.
- **Elenco di indirizzi bloccati**: all'utente non sarà consentito di accedere agli indirizzi indicati in questo elenco a meno che non siano anche presenti nell'elenco di indirizzi consentiti.

Per creare un nuovo elenco, fare clic su **Aggiungi**. Per eliminare gli elenchi selezionati, fare clic su **Rimuovi**.

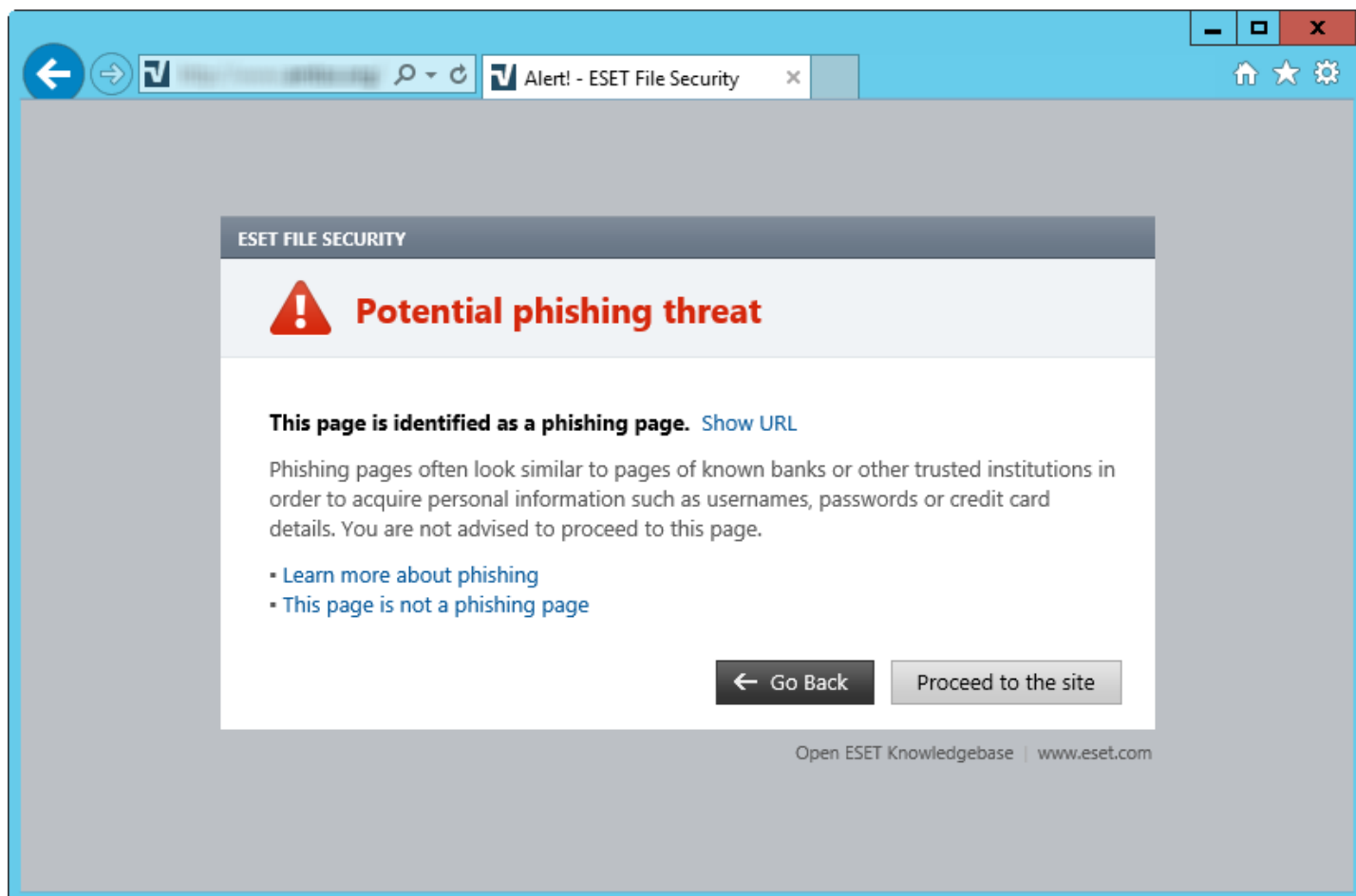
5.4.5 Protezione Anti-Phishing

Il termine phishing definisce un'attività illegale che si avvale dell'ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni riservate). Il phishing viene spesso utilizzato per ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via. Per ulteriori informazioni su questa attività, consultare il glossario. ESET Mail Security integra sistemi di protezione anti-phishing, ovvero una funzione che blocca pagine Web note per distribuire questo tipo di contenuto.

Si consiglia vivamente di attivare la funzione Anti-Phishing in ESET Mail Security. Per far ciò, aprire **Configurazione avanzata** (F5) > e accedere a **Web e e-mail** > **Protezione Anti-Phishing**.

Consultare l'articolo della Knowledge Base per ulteriori informazioni sulla protezione Anti-Phishing in ESET Mail Security.

Accesso a un sito Web phishing

Accedendo a un sito Web phishing riconosciuto, nel browser Web in uso comparirà la seguente finestra di dialogo. Se si desidera ancora accedere al sito Web, fare clic su **Vai al sito** (scelta non consigliata).

NOTA: per impostazione predefinita, i potenziali siti Web phishing che sono stati inseriti nella whitelist scadranno dopo alcune ore. Per consentire un sito Web in modo permanente, utilizzare lo strumento Gestione indirizzi URL. Da **Configurazione avanzata** (F5), espandere **Web e e-mail** > **Protezione accesso Web** > **Gestione indirizzi URL** > **Elenco indirizzi**, fare clic su **Modifica** e aggiungere nell'elenco il sito Web che si desidera modificare.

Segnalazione di un sito phishing

Il collegamento Segnala consente di segnalare un sito Web phishing/dannoso a ESET per l'analisi.

NOTA: prima di inviare un sito Web a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:

- il sito Web non viene rilevato
- il sito Web viene erroneamente rilevato come una minaccia. In questo caso, è possibile Segnalare un sito phishing falso positivo.

In alternativa, è possibile inviare il sito Web tramite e-mail. Inviare l'e-mail a samples@eset.com. Ricordare di utilizzare un oggetto descrittivo e di fornire il maggior numero di informazioni possibile sul sito Web (ad esempio, il sito Web che ha condotto l'utente sulla pagina in questione, come si è venuti a conoscenza del sito Web, ecc.).

5.5 Controllo dispositivi

ESET Mail Security offre un controllo automatico dei dispositivi (CD/DVD/USB). Questo modulo consente di controllare, bloccare o regolare le estensioni dei filtri o delle autorizzazioni e di definire la capacità dell'utente di accedere e di utilizzare un determinato dispositivo. Questa funzionalità potrebbe rivelarsi utile nel caso in cui l'amministratore di un computer desideri impedire l'utilizzo di dispositivi con contenuti non desiderati.

Dispositivi esterni supportati:

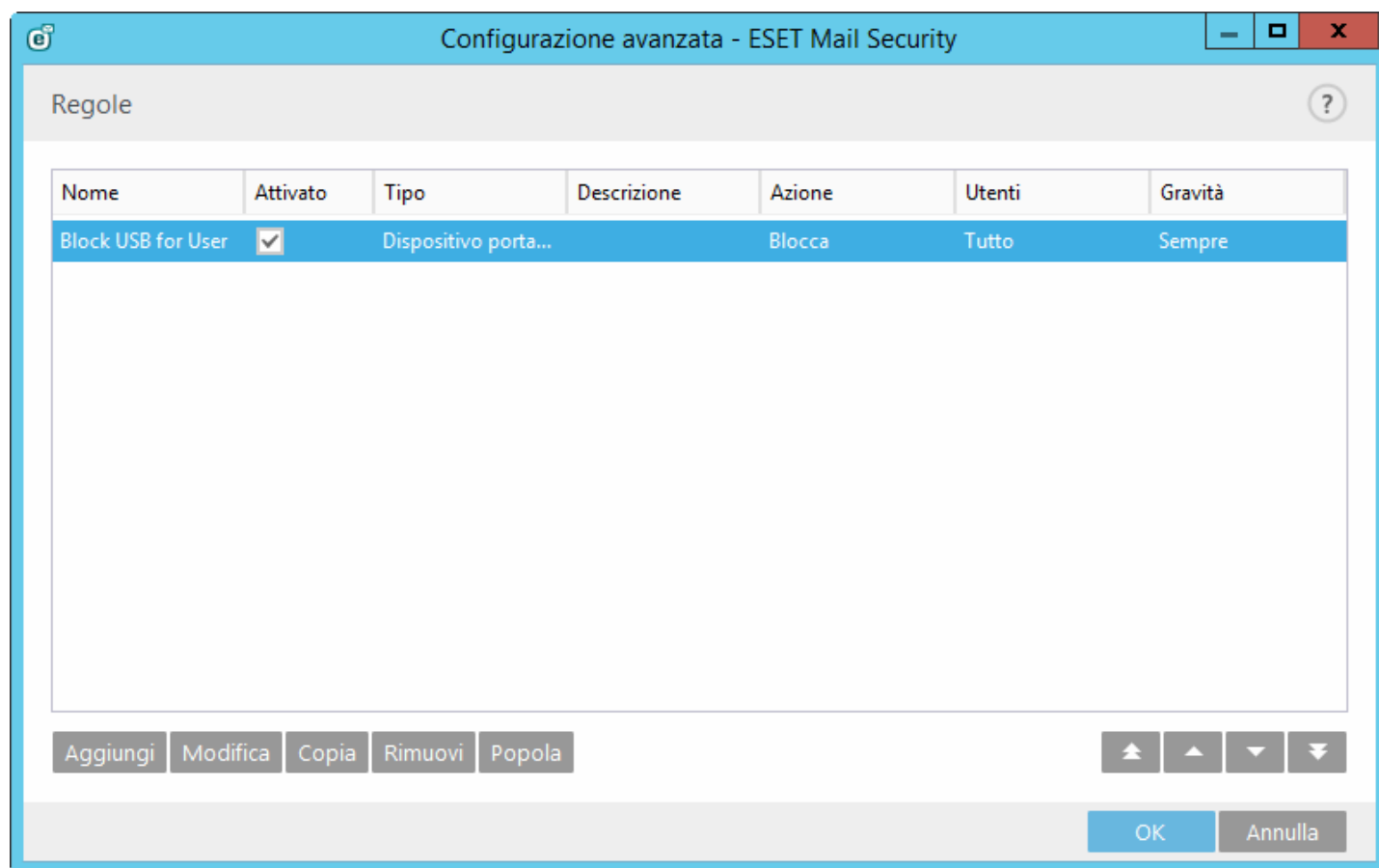
- Archiviazione su disco (HDD, disco rimovibile USB)
- CD/DVD
- Stampante USB
- Supporto di archiviazione FireWire
- Dispositivo Bluetooth
- Lettore schede Smart
- Dispositivo di acquisizione immagini
- Modem
- Porta LPT/COM
- Dispositivo portatile
- Tutti i tipi di dispositivi

Le opzioni di configurazione del controllo dispositivi possono essere modificate in **Configurazione avanzata** (F5) > **Controllo dispositivi**.

Attivando il pulsante accanto a **Integra nel sistema**, è possibile attivare la funzione Controllo dispositivi in ESET Mail Security. Per rendere effettiva questa modifica, sarà necessario riavviare il computer. Dopo aver attivato il Controllo dispositivi, si attiverà l'opzione **Editor regole**, che consentirà all'utente di aprire la finestra Editor regole.

In caso di inserimento di un dispositivo bloccato mediante una regola esistente, verrà visualizzata una finestra di notifica e l'accesso al dispositivo non verrà garantito.

5.5.1 Regole controllo dispositivi

Nella finestra **Editor regole controllo dispositivi**, in cui vengono visualizzate le regole esistenti, è possibile effettuare un controllo accurato dei dispositivi esterni collegati dagli utenti al computer.

È possibile consentire o bloccare specifici dispositivi in base all'utente, al gruppo di utenti o a un qualsiasi parametro aggiuntivo da specificare nella configurazione delle regole. L'elenco delle regole contiene varie descrizioni tra cui nome, tipo di dispositivo esterno, azione da eseguire dopo aver collegato un dispositivo esterno al computer e livello di gravità del rapporto.

Fare clic su **Aggiungi** o **Modifica** per gestire una regola. Fare clic su **Rimuovi** se si desidera eliminare la regola selezionata o deselezionare la casella di controllo **Attivata** accanto a una data regola per disattivarla. Questa opzione è utile se non si desidera eliminare definitivamente una regola in modo da poterla utilizzare in futuro.

Copia: crea una nuova regola in base ai parametri della regola selezionata.

Fare clic su **Popola** per popolare automaticamente i parametri dei supporti rimovibili per i dispositivi collegati al computer.

Le regole sono disposte in ordine di priorità, partendo da quelle con priorità più elevata. È possibile selezionare regole multiple e applicare azioni, come ad esempio l'eliminazione o lo spostamento in alto o in basso nell'elenco, facendo clic su **In alto/Su/Giù/In basso** (pulsanti delle frecce).

Le voci del rapporto possono essere visualizzate nella finestra principale del programma di ESET Mail Security in **Strumenti** > **File di rapporto**.

5.5.2 Aggiunta di regole per il controllo dispositivi

Una regola per il controllo dispositivi definisce l'azione che verrà intrapresa quando viene effettuata una connessione tra il computer e un dispositivo che soddisfa i criteri della regola.

Inserire una descrizione della regola nel campo **Nome** per consentire una migliore identificazione. Fare clic sul pulsante accanto a **Regola attivata** per disattivare o attivare questa regola. Questa opzione può essere utile se non si desidera eliminare definitivamente la regola.

Tipo di dispositivo

Scegliere il tipo di dispositivo esterno dal menu a discesa (Archiviazione su disco/Dispositivo portatile/Bluetooth/ FireWire/...). I tipi di dispositivi vengono ereditati dal sistema operativo e possono essere visualizzati in Gestione dispositivi del sistema, ipotizzando che un dispositivo sia collegato al computer. I supporti di archiviazione includono dischi esterni o lettori tradizionali di schede di memoria collegati tramite USB o FireWire. I lettori di smart card includono circuiti integrati incorporati, come ad esempio schede SIM o schede di autenticazione. Esempi di dispositivi di acquisizione immagini sono gli scanner o le fotocamere, che non forniscono informazioni sugli utenti, ma solo sulle azioni. Ciò implica che i dispositivi di acquisizione immagini possono essere bloccati solo a livello globale.

Azione

È possibile consentire o bloccare l'accesso ai dispositivi non adatti all'archiviazione. Le regole dei dispositivi di archiviazione consentono invece all'utente di scegliere uno dei seguenti diritti:

- **Lettura/Scrittura**: sarà consentito l'accesso completo al dispositivo.
- **Blocca**: l'accesso al supporto verrà bloccato.

- **Solo lettura**: sul dispositivo sarà consentito l'accesso di sola lettura.
- **Avvisa**: tutte le volte che un dispositivo effettua la connessione, all'utente verrà inviata una notifica che lo avvisa in merito all'eventuale autorizzazione/blocco e verrà creata una voce di rapporto. Poiché i dispositivi non vengono memorizzati, l'utente visualizzerà sempre una notifica relativa alle successive connessioni di uno stesso dispositivo.

Tenere presente che non sono disponibili tutti i diritti (azioni) per tutti i tipi di dispositivi. Se su un dispositivo è presente spazio di archiviazione, saranno disponibili tutte e quattro le azioni. Per i dispositivi non di archiviazione, sono disponibili solo due azioni (ad esempio, l'azione **Solo lettura** non è disponibile per il sistema Bluetooth. Ciò significa che i dispositivi Bluetooth possono essere solo consentiti o bloccati).

I parametri aggiuntivi visualizzati di seguito possono essere utilizzati per ottimizzare le regole e personalizzarle in base ai dispositivi in uso. Tutti i parametri non fanno distinzione tra lettere maiuscole e minuscole:

- **Fornitore**: filtraggio in base al nome o all'identificativo del fornitore.
- **Modello**: nome specifico del dispositivo.
- **Numero di serie**: generalmente, a ogni dispositivo esterno è associato un numero di serie. Nel caso di CD/DVD, il numero di serie è associato al supporto specifico e non all'unità CD.

NOTA: se le tre descrizioni sono vuote, durante la ricerca delle corrispondenze la regola ignorerà tali campi. I parametri di filtraggio in tutti i campi testuali non distinguono tra maiuscole e minuscole e i caratteri jolly (*, ?) non sono supportati.

Suggerimento: per trovare i parametri di un dispositivo, creare una regola che autorizzi il tipo di dispositivo, collegare il dispositivo al computer in uso, quindi rivedere i dettagli del dispositivo in Rapporto controllo dispositivi.

Gravità

- **Sempre** : registra tutti gli eventi.
- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma.
- **Informazioni**: registra i messaggi informativi, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Allarme**: registra errori critici e messaggi di allarme.
- **Nessuno**: non verrà registrato alcun rapporto.

Le regole possono essere limitate a determinati utenti o gruppi di utenti aggiunti all'**Elenco utenti**:

- **Aggiungi**: apre la finestra di dialogo **Tipi di oggetto: Utenti o Gruppi**, che consente di selezionare gli utenti desiderati.
- **Rimuovi**: rimuove l'utente selezionato dal filtro.

i **NOTA**: tutti i dispositivi possono essere filtrati dalle regole dell'utente (ad esempio, i dispositivi di acquisizione di immagini non forniscono informazioni sugli utenti, ma solo sulle azioni richiamate).

5.5.3 Dispositivi rilevati

Il pulsante **Popola** fornisce una panoramica di tutti i dispositivi attualmente connessi contenenti le seguenti informazioni: tipo di dispositivo, fornitore del dispositivo, modello e numero di serie (se disponibili). Dopo aver selezionato un dispositivo (dall'elenco di dispositivi rilevati) e aver fatto clic su **OK**, si aprirà una finestra di editor regole contenente le informazioni predefinite (è possibile modificare tutte le impostazioni).

5.5.4 Gruppi dispositivi

 Il dispositivo connesso al computer in uso potrebbe rappresentare un potenziale rischio per la sicurezza.

La finestra Gruppi dispositivi è suddivisa in due parti. La parte destra contiene un elenco di dispositivi appartenenti al gruppo di riferimento e la parte sinistra un elenco di gruppi esistenti. Selezionare il gruppo contenente i dispositivi che si desidera visualizzare nel riquadro di destra.

Aprendo la finestra Gruppi dispositivi e selezionando un gruppo, è possibile aggiungere o rimuovere dispositivi dall'elenco. Un altro modo per aggiungere dispositivi nel gruppo consiste nell'importazione degli stessi da un file. In alternativa, è possibile fare clic su **Popola**, che consente di inserire tutti i dispositivi connessi al computer in uso nella finestra **Dispositivi rilevati**. Selezionare un dispositivo dall'elenco per aggiungerlo al gruppo facendo clic su **OK**.

Elementi di controllo

Aggiungi: è possibile aggiungere un gruppo inserendone il nome oppure un dispositivo a un gruppo esistente (facoltativamente, è possibile specificare alcuni dettagli, come il nome del fornitore, il modello e il numero di serie) in base al punto della finestra in cui è stato premuto il pulsante.

Modifica: consente all'utente di modificare il nome di un gruppo selezionato o i parametri dei dispositivi in esso contenuti (fornitore, modello, numero di serie).

Rimuovi: elimina il gruppo o il dispositivo scelto in base al punto della finestra selezionato dall'utente.

Importa: importa un elenco di dispositivi da un file.

Il pulsante **Popola** fornisce una panoramica di tutti i dispositivi attualmente connessi contenenti le seguenti informazioni: tipo di dispositivo, fornitore del dispositivo, modello e numero di serie (se disponibili).

Una volta completata la personalizzazione, fare clic su **OK**. Fare clic su **Annulla** se si desidera abbandonare la finestra **Gruppi dispositivi** senza salvare le modifiche.

SUGGERIMENTO: è possibile creare vari gruppi di dispositivi ai quali verranno applicate regole diverse. È inoltre possibile creare solo un gruppo di dispositivi per i quali verrà applicata la regola con l'azione **Lettura/Scrittura** o **Solo lettura**. Ciò consente al Controllo dispositivi di bloccare i dispositivi non riconosciuti che si connettono al computer in uso.

Tenere presente che non sono disponibili tutte le azioni (autorizzazioni) per tutti i tipi di dispositivi. Per i dispositivi di archiviazione, sono disponibili tutte e quattro le azioni. Per i dispositivi non di archiviazione, sono disponibili solo tre azioni (ad esempio, l'azione **Solo lettura** non è disponibile per il sistema Bluetooth. Ciò significa che i dispositivi Bluetooth possono essere solo consentiti, bloccati o avvisati).

5.6 Strumenti

Nello spazio sottostante sono indicate le impostazioni avanzate di tutti gli strumenti offerti da ESET Mail Security nella scheda **Strumenti** della finestra principale dell'interfaccia utente grafica (GUI).

5.6.1 ESET Live Grid

ESET Live Grid è un sistema avanzato di allarme immediato basato su diverse tecnologie cloud che consente di rilevare minacce emergenti in base alla reputazione e di migliorare le prestazioni del controllo attraverso l'utilizzo di sistemi di whitelist. Le informazioni sulle nuove minacce vengono inserite in flussi in tempo reale indirizzati verso il cloud, che consentono al laboratorio di ricerca di malware ESET di offrire risposte tempestive e un livello di protezione costante. Gli utenti possono controllare la reputazione dei processi in esecuzione e dei file direttamente dall'interfaccia del programma o dal menu contestuale. Ulteriori informazioni sono disponibili su ESET Live Grid. Durante l'installazione di ESET Mail Security, selezionare una delle seguenti opzioni:

1. È possibile decidere di non attivare ESET Live Grid. Il software non perderà alcuna funzionalità ma, in alcuni casi, ESET Mail Security potrebbe rispondere più lentamente alle nuove minacce rispetto all'aggiornamento del database delle firme antivirali.
2. È possibile configurare ESET Live Grid per l'invio di informazioni anonime sulle nuove minacce e laddove sia stato rilevato il nuovo codice dannoso. Il file può essere inviato a ESET per un'analisi dettagliata. Lo studio di queste minacce sarà d'aiuto a ESET per aggiornare le proprie capacità di rilevamento.

ESET Live Grid raccoglierà informazioni sul computer dell'utente in relazione alle nuove minacce rilevate. Tali informazioni possono includere un campione o una copia del file in cui è contenuta la minaccia, il percorso al file, il nome del file, informazioni su data e ora, il processo in base al quale la minaccia è apparsa sul computer e informazioni sul sistema operativo del computer.

Per impostazione predefinita, ESET Mail Security è configurato per l'invio dei file sospetti ai laboratori antivirus ESET ai fini di un'analisi dettagliata. Sono sempre esclusi file con specifiche estensioni, ad esempio *DOC* o *XLS*. È inoltre possibile aggiungere altre estensioni in presenza di specifici file che l'utente o la società dell'utente non desidera inviare.

Il sistema di reputazione ESET Live Grid utilizza metodi di whitelist e blacklist basati sul cloud. Per accedere alle impostazioni di ESET Live Grid, premere F5 per aprire la Configurazione avanzata ed espandere **Strumenti** > **ESET Live Grid**.

Attiva il sistema di reputazione ESET Live Grid (scelta consigliata): il sistema di reputazione ESET Live Grid potenzia le prestazioni delle soluzioni anti-malware ESET eseguendo un confronto tra i file controllati e un database di oggetti inseriti nelle whitelist o nelle blacklist all'interno del cloud.

Invia statistiche anonime: consente a ESET di raccogliere informazioni sulle nuove minacce rilevate, tra cui il nome della minaccia, la data e l'ora del rilevamento, il metodo di rilevamento e i metadati associati, la versione e la configurazione del prodotto, incluse le informazioni sul sistema in uso.

Invia file: i file sospetti simili alle minacce e/o i file con caratteristiche o comportamenti insoliti vengono inviati a ESET ai fini dell'analisi.

Selezionare **Attiva registrazione** per creare un rapporto di eventi sul quale vengono registrati gli invii dei file e delle informazioni statistiche. Ciò attiverà la registrazione sul Rapporto eventi dell'invio di file o statistiche.

Contatto e-mail (facoltativo): il contatto e-mail può essere incluso insieme ai file sospetti e utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. Tenere presente che non si riceverà alcuna risposta da ESET, a meno che non siano richieste ulteriori informazioni.

Esclusione: il filtro esclusioni consente all'utente di escludere alcuni file o alcune cartelle dall'invio (ad esempio, potrebbe essere utile escludere i file contenenti informazioni riservate, come documenti o fogli di calcolo). I file elencati non verranno mai inviati ai laboratori ESET per l'analisi, anche se contengono codici sospetti. Per impostazione predefinita, vengono esclusi i tipi di file più comuni (.doc, ecc.). Se lo si desidera, è possibile aggiungerli all'elenco di file esclusi.

Se ESET Live Grid è già stato utilizzato in precedenza ed è stato disattivato, potrebbero essere ancora presenti pacchetti di dati da inviare. I pacchetti verranno inviati a ESET anche dopo la disattivazione. Dopo l'invio delle informazioni correnti, non verranno creati ulteriori pacchetti.

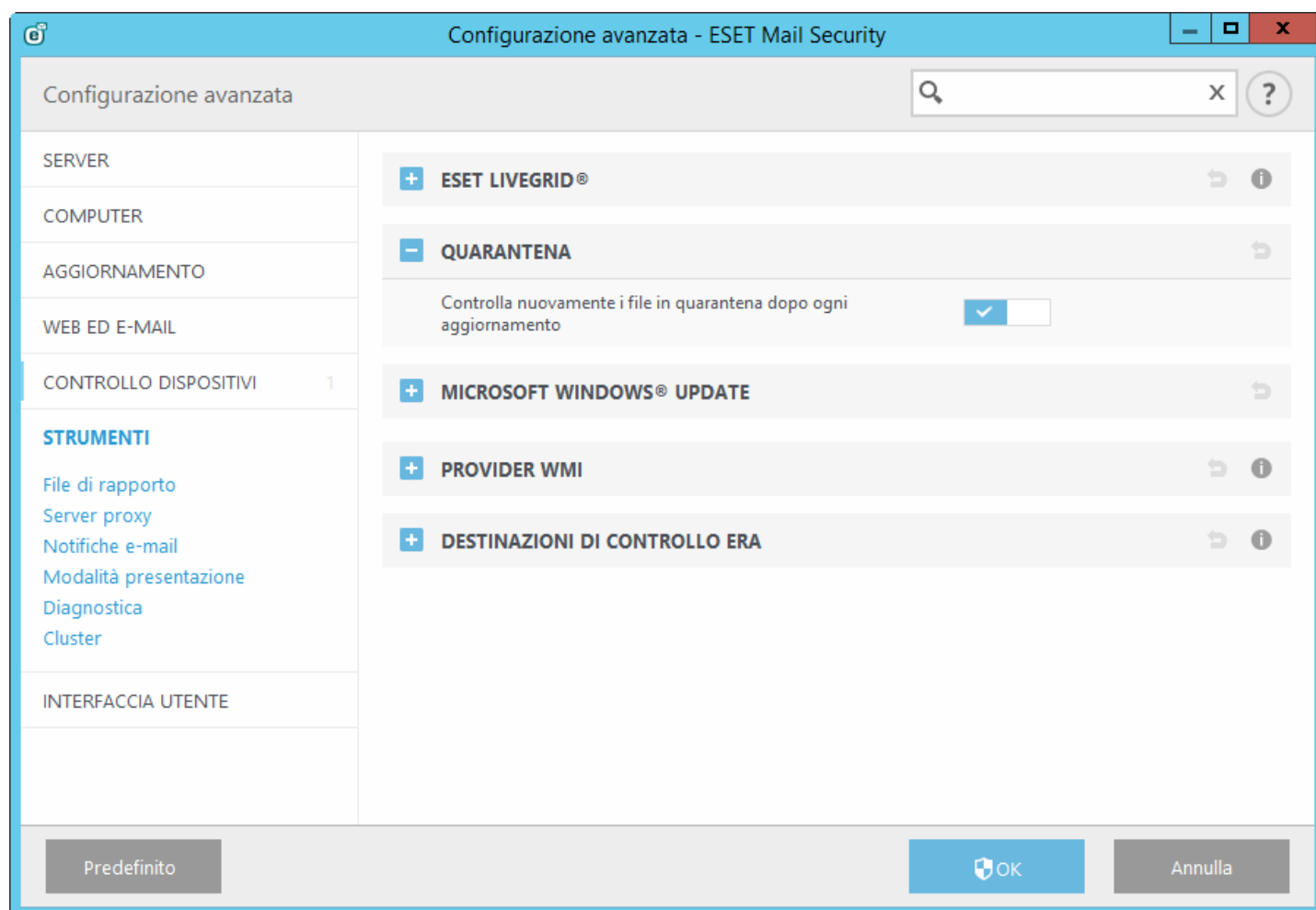
5.6.1.1 Filtro esclusione

L'opzione **Modifica** accanto a Esclusioni in ESET Live Grid consente all'utente di configurare le modalità di invio delle minacce ai laboratori antivirus ESET per l'analisi.

Se si rileva un file sospetto, è possibile inviarlo per l'analisi ai laboratori delle minacce. Se viene individuata un'applicazione dannosa, essa verrà aggiunta al successivo aggiornamento delle firme antivirali.

5.6.2 Quarantena

Nella cartella Quarantena vengono archiviati i file infetti o sospetti in forma benigna. Per impostazione predefinita, il modulo di protezione in tempo reale mette in quarantena tutti i file sospetti appena creati allo scopo di evitare infezioni.

Ripeti controllo dei file in quarantena dopo ogni aggiornamento: tutti gli oggetti in quarantena verranno sottoposti a controllo dopo ogni aggiornamento del database delle firme antivirali. Questa opzione risulta particolarmente utile nel caso in cui un file sia stato spostato in quarantena in seguito al risultato del rilevamento di un falso positivo. Quando questa opzione è attiva, alcuni tipi di file possono essere ripristinati automaticamente nella posizione originale.

5.6.3 Aggiornamento Microsoft Windows

Gli aggiornamenti di Windows offrono importanti correzioni a pericolose vulnerabilità potenziali e migliorano il livello di protezione generale del computer dell'utente. Per questo motivo, è fondamentale installare gli aggiornamenti di Microsoft Windows non appena disponibili. ESET Mail Security invia notifiche all'utente relative agli aggiornamenti mancanti in base al livello specificato. Sono disponibili i livelli seguenti:

- **Nessun aggiornamento**: non viene offerto alcun aggiornamento del sistema da scaricare.
- **Aggiornamenti facoltativi**: vengono offerti aggiornamenti con priorità bassa e di livello superiore da scaricare.
- **Aggiornamenti consigliati**: vengono offerti aggiornamenti contrassegnati come comuni o di livello superiore da scaricare.
- **Aggiornamenti importanti**: vengono offerti aggiornamenti contrassegnati come importanti o di livello superiore da scaricare.
- **Aggiornamenti critici**: vengono offerti unicamente gli aggiornamenti critici da scaricare.

Fare clic su **OK** per salvare le modifiche. Dopo la verifica dello stato mediante il server di aggiornamento, viene visualizzata la finestra Aggiornamenti del sistema. Le informazioni sull'aggiornamento del sistema potrebbero non essere disponibili subito dopo il salvataggio delle modifiche.

5.6.4 Provider WMI

Informazioni su WMI

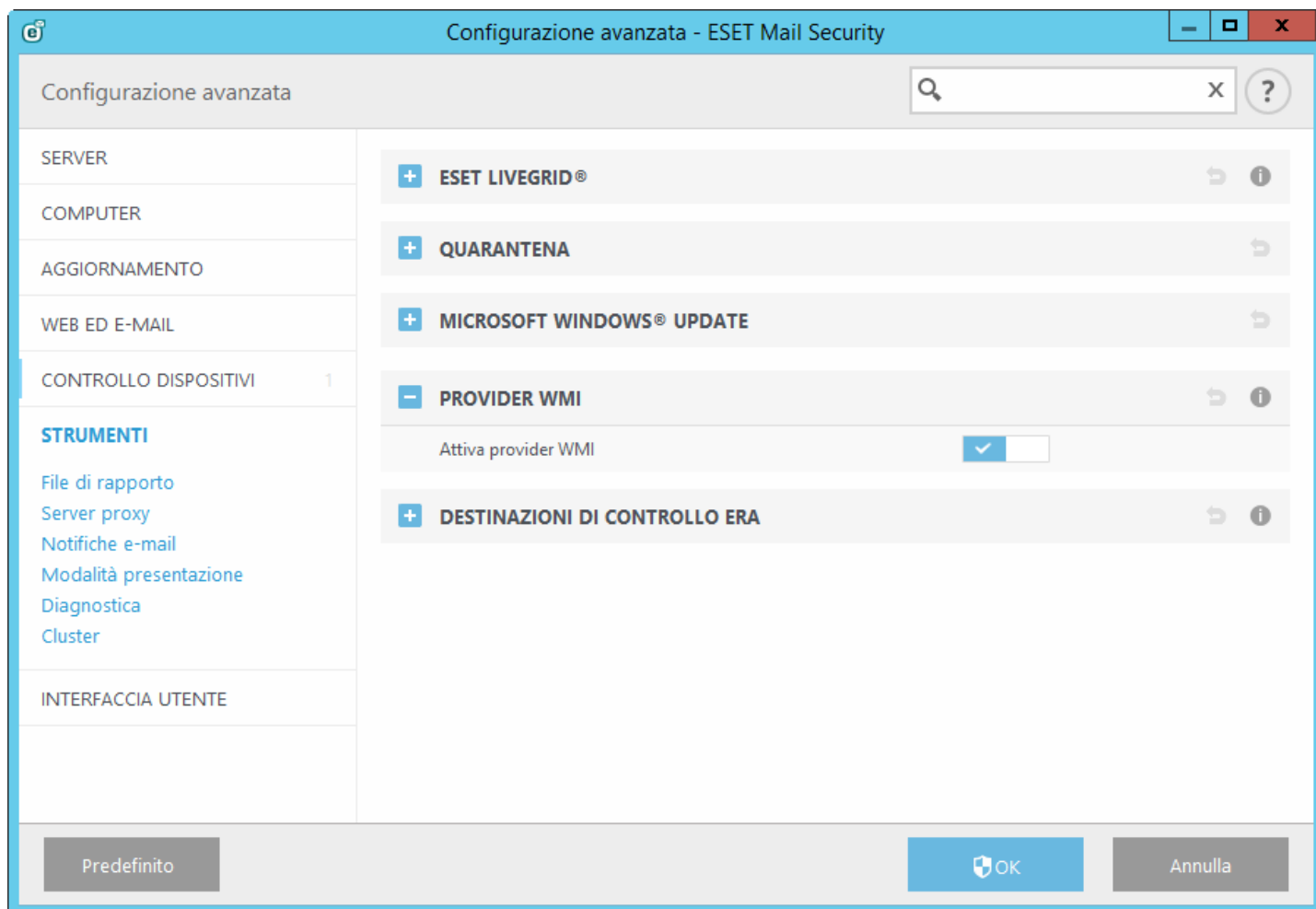
Windows Management Instrumentation (WMI) è l'implementazione Microsoft di Web-Based Enterprise Management (WBEM), ovvero un'iniziativa industriale basata sullo sviluppo di una tecnologia standard per l'accesso alle informazioni di gestione in un ambiente aziendale.

Per ulteriori informazioni su WMI, consultare http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

ESET WMI Provider

ESET WMI Provider è stato concepito allo scopo di garantire il monitoraggio remoto dei prodotti ESET in un ambiente aziendale senza la necessità di utilizzare software o strumenti ESET. L'offerta di informazioni di base sul prodotto, sullo stato e sulele statistiche attraverso WMI consente a ESET di ampliare notevolmente le possibilità degli amministratori aziendali durante il monitoraggio dei prodotti ESET. Gli amministratori possono usufruire dei numerosi metodi di accesso offerti da WMI (riga di comando, script e strumenti di monitoraggio aziendali di terze parti) per monitorare lo stato dei propri prodotti ESET.

L'implementazione corrente offre un accesso di sola lettura alle informazioni di base sul prodotto, alle funzioni installate e al relativo stato di protezione, alle statistiche dei singoli scanner e ai file dei rapporti dei prodotti.

Il provider WMI consente di utilizzare l'infrastruttura e gli strumenti Windows WMI standard per la lettura dello stato e dei rapporti del prodotto.

5.6.4.1 Dati forniti

Tutte le classi WMI correlate al prodotto ESET sono posizionate nello spazio dei nomi "root\ESET". Le seguenti classi, descritte in modo più approfondito nello spazio sottostante, sono attualmente implementate:

Generale:

- ESET_Product
- ESET_Features
- ESET_Statistics

Rapporti:

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_GreylistLog
- ESET_SpamLog

Classe ESET_Product

Esiste solo un'istanza della classe ESET_Product. Le proprietà di questa classe fanno riferimento alle informazioni di base sul prodotto ESET installato:

- **ID**: identificatore del tipo di prodotto, ad esempio, "essbe"
- **Name**: nome del prodotto, ad esempio, "ESET Security"
- **Edition**: edizione del prodotto, ad esempio, "Microsoft SharePoint Server"
- **Version**: versione del prodotto, ad esempio, "4.5.15013.0"
- **VirusDBVersion**: versione del database delle firme antivirali, ad esempio, "7868 (20130107)"
- **VirusDBLastUpdate**: indicatore della data e dell'ora dell'ultimo aggiornamento del database delle firme antivirali. La stringa contiene l'indicatore della data e dell'ora nel formato dataora WMI, ad esempio, "20130118115511.000000+060"
- **LicenseExpiration**: data di scadenza della licenza. La stringa contiene l'indicatore della data e dell'ora nel formato dataora WMI, ad esempio, "20130118115511.000000+060"
- **KernelRunning**: valore booleano che indica se il servizio eKrn è in esecuzione sulla macchina, ad esempio, "VERO"
- **StatusCode**: numero che indica lo stato di protezione del prodotto: 0: verde (OK), 1: giallo (Avviso), 2: rosso (Errore)
- **StatusText**: messaggio che descrive il motivo alla base di un codice di stato diverso da zero; in caso contrario, il valore è null

Classe ESET_Features

La classe ESET_Features presenta istanze multiple, in base al numero delle funzioni del prodotto. Ciascuna istanza contiene:

- **Name**: nome della funzione (l'elenco dei nomi è fornito nella sezione sottostante)
- **Status**: stato della funzione: 0: inattiva, 1: disattivata, 2: attivata

Elenco di stringhe che rappresentano le funzioni del prodotto attualmente riconosciute:

- **CLIENT_FILE_AV**: protezione antivirus file system in tempo reale
- **CLIENT_WEB_AV**: protezione antivirus del client di posta
- **CLIENT_DOC_AV**: protezione antivirus dei documenti del client
- **CLIENT_NET_FW**: rapporto del Personal Firewall del client
- **CLIENT_EMAIL_AV**: protezione antivirus del client di posta
- **CLIENT_EMAIL_AS**: protezione antispam delle e-mail del client
- **SERVER_FILE_AV**: protezione antivirus in tempo reale dei file sul server dei file protetti, ad esempio, file presenti nel database dei contenuti di SharePoint nel caso di ESET Mail Security
- **SERVER_EMAIL_AV**: protezione antivirus delle e-mail del prodotto server, ad esempio, e-mail in MS Exchange o IBM Lotus Domino
- **SERVER_EMAIL_AS**: protezione antispam delle e-mail del prodotto server, ad esempio, e-mail in MS Exchange o IBM Lotus Domino
- **SERVER_GATEWAY_AV**: protezione antivirus dei protocolli delle reti protette sul gateway
- **SERVER_GATEWAY_AS**: protezione antispam dei protocolli delle reti protette sul gateway

Classe ESET_Statistics

La classe ESET_Statistics presenta istanze multiple, in base al numero di scanner presenti nel prodotto. Ciascuna istanza contiene:

- Scanner: codice della stringa per un particolare scanner, ad esempio, "CLIENT_FILE"
- Total: numero totale di file controllati
- Infected: numero di file infetti trovati
- Cleaned: numero di file puliti
- Timestamp: indicatore della data e dell'ora dell'ultima modifica di questa statistica. Espresso nel formato dataora WMI, ad esempio, "20130118115511.000000+060"
- ResetTime: indicatore della data e dell'ora dell'ultimo azzeramento del contatore di statistiche. Espresso nel formato dataora WMI, ad esempio, "20130118115511.000000+060"

Elenco di stringhe che rappresentano gli scanner attualmente riconosciuti:

- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

Classe ESET_ThreatLog

La classe ESET_ThreatLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto "Minacce rilevate". Ciascuna istanza contiene:

- **ID**: ID univoco di questo record di rapporto
- **Timestamp**: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- **LogLevel**: livello di gravità del record di rapporto espresso come numero nell'intervallo [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- **Scanner**: nome dello scanner che ha creato questo evento del rapporto
- **ObjectType**: tipo di oggetto che ha prodotto questo evento del rapporto
- **ObjectName**: nome dell'oggetto che ha prodotto questo evento del rapporto
- **Threat**: nome della minaccia che è stata trovata nell'oggetto descritto dalle proprietà ObjectName e ObjectType
- **Action**: azione eseguita in seguito all'identificazione della minaccia
- **User**: account utente che ha causato la generazione di questo evento di rapporto
- **Information**: descrizione aggiuntiva dell'evento

ESET_EventLog

La classe ESET_EventLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto "Eventi". Ciascuna istanza contiene:

- **ID**: ID univoco di questo record di rapporto
- **Timestamp**: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- **LogLevel**: livello di gravità del record di rapporto espresso come numero nell'intervallo [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- **Module**: nome del modulo che ha creato questo evento del rapporto
- **Event**: descrizione dell'evento
- **User**: account utente che ha causato la generazione di questo evento di rapporto

ESET_ODFileScanLogs

La classe ESET_ODFileScanLogs presenta istanze multiple e ciascuna di esse rappresenta un record di controllo dei file su richiesta. Tale funzione equivale all'elenco di rapporti "Controllo computer su richiesta" della GUI. Ciascuna istanza contiene:

- **ID**: ID univoco di questo rapporto su richiesta
- **Timestamp**: creazione dell'indicatore della data e dell'ora del rapporto (nel formato data/ora WMI)
- **Targets**: cartelle/oggetti di destinazione del controllo
- **TotalScanned**: numero totale degli oggetti controllati
- **Infected**: numero di oggetti infetti trovati
- **Cleaned**: numero di oggetti puliti
- **Status**: stato del processo di controllo

ESET_ODFileScanLogRecords

La classe ESET_ODFileScanLogRecords presenta istanze multiple e ciascuna di esse rappresenta un record di uno dei rapporti di controllo rappresentati dalle istanze della classe ESET_ODFileScanLogs. Le istanze di questa classe offrono record di rapporto di tutti i controlli/rapporti su richiesta. Se sono richieste solo le istanze di uno specifico rapporto di controllo, è necessario filtrarle in base alla proprietà LogID. Ciascuna istanza della classe contiene:

- **LogID**: ID del rapporto di controllo a cui appartiene questo record (ID di una delle istanze della classe ESET_ODFileScanLogs)
- **ID**: ID univoco di questo record di rapporto del controllo
- **Timestamp**: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- **LogLevel**: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- **Log**: messaggio del rapporto effettivo

ESET_ODServerScanLogs

La classe ESET_ODServerScanLogs presenta istanze multiple e ciascuna di esse rappresenta un'esecuzione del controllo del server su richiesta. Ciascuna istanza contiene:

- **ID**: ID univoco di questo rapporto su richiesta
- **Timestamp**: creazione dell'indicatore della data e dell'ora del rapporto (nel formato data/ora WMI)
- **Targets**: cartelle/oggetti di destinazione del controllo
- **TotalScanned**: numero totale degli oggetti controllati
- **Infected**: numero di oggetti infetti trovati
- **Cleaned**: numero di oggetti puliti
- **RuleHits**: numero totale di attivazioni della regola
- **Status**: stato del processo di controllo

ESET_ODServerScanLogRecords

La classe ESET_ODServerScanLogRecords presenta istanze multiple e ciascuna di esse rappresenta un record di uno dei rapporti di controllo rappresentati dalle istanze della classe ESET_ODServerScanLogs. Le istanze di questa classe offrono record di rapporto di tutti i controlli/rapporti su richiesta. Se sono richieste solo le istanze di uno specifico rapporto di controllo, è necessario filtrarle in base alla proprietà LogID. Ciascuna istanza della classe contiene:

- **LogID**: ID del rapporto di controllo a cui appartiene questo record (ID di una delle istanze della classe ESET_ ODServerScanLogs)
- **ID**: ID univoco di questo record di rapporto del controllo
- **Timestamp**: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- **LogLevel**: livello di gravità del record di rapporto espresso come numero nell'intervallo [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- **Log**: messaggio del rapporto effettivo

ESET_GreylistLog

La classe ESET_GreylistLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto "Greylist". Ciascuna istanza contiene:

- **ID**: ID univoco di questo record di rapporto
- **Timestamp**: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- **LogLevel**: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- **HELODomain**: nome del dominio HELO
- **IP**: indirizzo IP di origine
- **Sender**: mittente dell'e-mail
- **Recipient**: destinatario dell'e-mail
- **Action**: azione eseguita
- **TimeToAccept**: numero di minuti in seguito ai quali l'e-mail verrà accettata

ESET_SpamLog

La classe ESET_SpamLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto "Spamlog". Ciascuna istanza contiene:

- **ID**: ID univoco di questo record di rapporto
- **Timestamp**: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- **LogLevel**: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- **Sender**: mittente dell'e-mail
- **Recipients**: destinatari dell'e-mail
- **Subject**: oggetto dell'e-mail
- **Received**: ora della ricezione
- **Score**: punteggio spam espresso in percentuale [0-100]
- **Reason**: motivo in base al quale questa e-mail è stata contrassegnata come spam
- **Action**: azione eseguita
- **DiagInfo**: informazioni diagnostiche aggiuntive

5.6.4.2 Accesso ai dati forniti

Seguono alcuni esempi delle modalità di accesso ai dati ESET WMI dalla riga di comando Windows e PowerShell, che dovrebbero funzionare da qualsiasi sistema operativo Windows attualmente disponibile. Esistono, tuttavia, numerosi altri modi per accedere ai dati a partire da altri linguaggi e strumenti di scripting.

Riga di comando senza script

Lo strumento della riga di comando `wmic` può essere utilizzato per accedere a varie classi predefinite o classi WMI personalizzate.

Per visualizzare informazioni complete sul prodotto sulla macchina locale:
```
wmic /namespace:\\root\ESET Path ESET_Product
```

Per visualizzare solo il numero della versione del prodotto sulla macchina locale:
```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Per visualizzare informazioni complete sul prodotto su una macchina remota con IP 10.1.118.180:
```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Per ottenere e visualizzare informazioni complete sul prodotto sulla macchina locale:
```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Per ottenere e visualizzare informazioni complete sul prodotto su una macchina remota con IP 10.1.118.180:

```
$cred = Get-Credential          # richiede all'utente di fornire le credenziali e le archivia nella variab
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred $cred
```

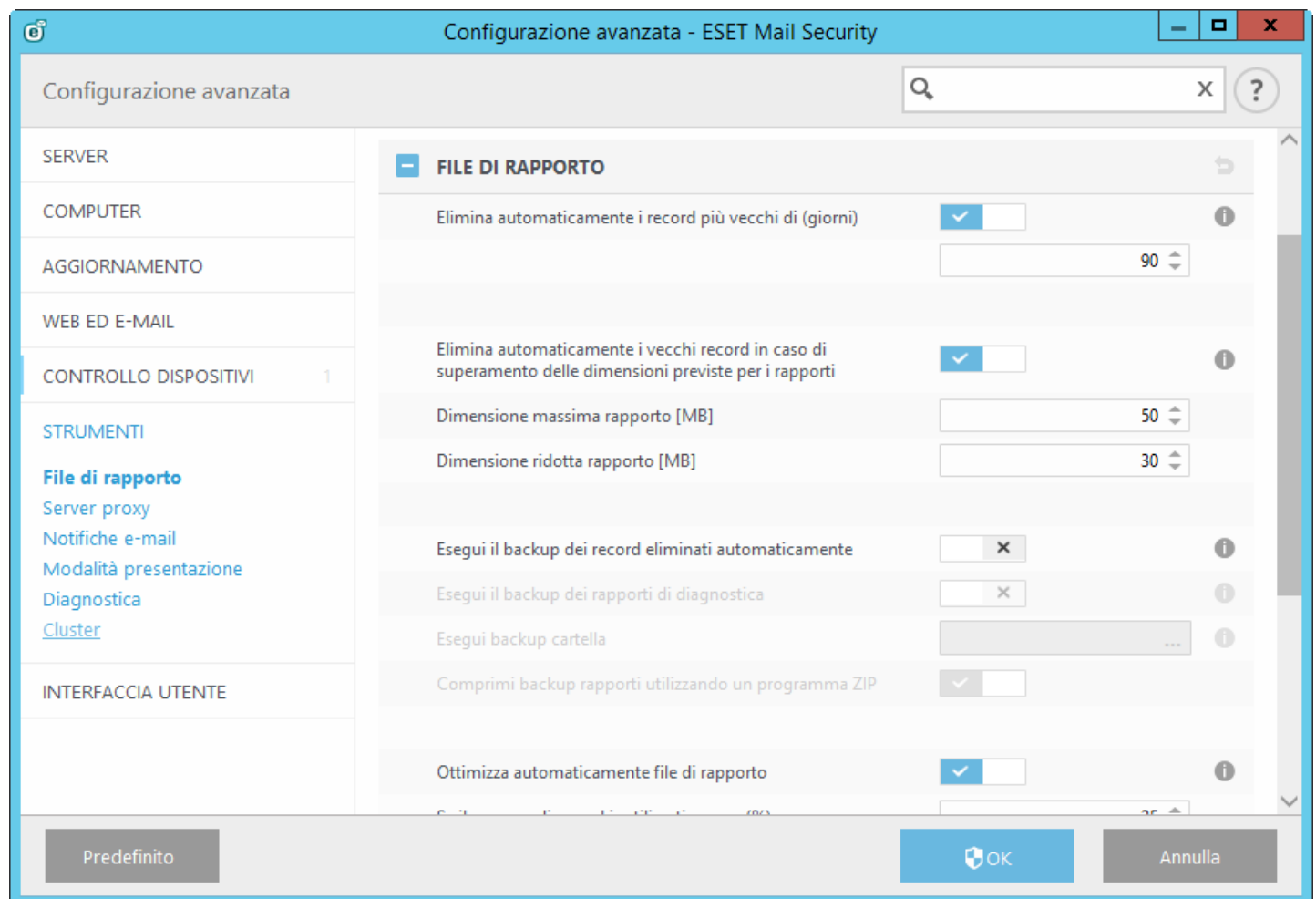
5.6.5 Destinazioni di controllo ERA

Questa funzionalità consente a ESET Remote Administrator di utilizzare le Destinazioni di controllo su richiesta appropriate quando è in esecuzione un'attività client **Controllo server** su un server con ESET Mail Security.

Quando si attiva la funzionalità **Genera elenco destinazioni**, ESET Mail Security crea un elenco delle destinazioni di controllo attualmente disponibili. L'elenco viene generato periodicamente in base al **Periodo di aggiornamento** definito in minuti. Quando ERA desidera eseguire l'attività client **Controllo server**, recupera l'elenco e consente all'utente di scegliere le destinazioni di controllo per il Controllo su richiesta su tale server specifico.

5.6.6 File di rapporto

La configurazione della registrazione di ESET Mail Security è accessibile dalla finestra principale del programma.

Fare clic su **Configurazione** > **Configurazione avanzata** > **Strumenti** > **File di rapporto**. La sezione relativa ai rapporti viene utilizzata per definire come verranno gestiti. Il programma elimina automaticamente i rapporti meno recenti per liberare spazio sull'unità disco rigido.

5.6.6.1 Filtraggio rapporti

Nei rapporti sono memorizzate le informazioni relative a eventi importanti di sistema. La funzione di filtraggio dei rapporti consente di visualizzare i record di un determinato tipo di evento.

Immettere la parola chiave da ricercare nel campo **Trova testo**. Utilizzare il menu a discesa **Cerca nelle colonne** per perfezionare la ricerca.

Tipi di record: scegliere uno o più tipi di rapporti dei record dal menu a discesa:

- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativo**: registra i messaggi informativi, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Allarmi**: registra errori critici e messaggi di allarme.
- **Errori**: verranno registrati errori quali "Errore durante il download del file" ed errori critici.
- **Critico**: registra solo gli errori critici (errore che avvia la protezione antivirus).

Periodo: indicare l'intervallo di tempo rispetto al quale si desiderano visualizzare i risultati.

Solo parole intere: selezionare questa casella di controllo per ricercare specifiche parole intere e ottenere risultati più precisi.

Maiuscole/minuscole: attivare questa opzione se è importante utilizzare lettere maiuscole o minuscole durante l'applicazione del filtro.

5.6.6.2 Trova nel rapporto

Oltre alla funzione Filtraggio dei rapporti, è possibile utilizzare la funzionalità di ricerca all'interno dei file di rapporto che può essere utilizzata indipendentemente dal filtraggio dei rapporti. Si tratta di una funzionalità utile se si desidera ricercare particolari record nei rapporti. Al pari del Filtraggio rapporti, questa funzionalità di ricerca aiuta a trovare le informazioni che si stanno ricercando, soprattutto se è presente un numero elevato di record.

Durante l'utilizzo della funzione di ricerca nel rapporto, è possibile **Trovare il testo** digitando una stringa specifica, utilizzare il menu a discesa **Cerca nelle colonne** per filtrare in base alla colonna, selezionare **Tipi di record** e impostare un **Periodo di tempo** per ricercare esclusivamente i record a partire da uno specifico periodo di tempo. Specificando alcune opzioni di ricerca, nella finestra File di rapporto vengono visualizzati solo i record pertinenti in base alle opzioni di ricerca.

Trova testo:: digitare una stringa (parola o parte di una parola). Verranno trovati solo i record contenenti tale stringa. Gli altri record verranno omessi.

Cerca nelle colonne:: selezionare le colonne in cui eseguire la ricerca. È possibile selezionare una o più colonne da utilizzare per la ricerca. Per impostazione predefinita, sono selezionate tutte le colonne:

- **Ora**
- **Cartella controllata**
- **Evento**
- **Utente**

Tipi di record: scegliere uno o più tipi di rapporti dei record dal menu a discesa:

- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativo**: registra i messaggi informativi, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Allarmi**: registra errori critici e messaggi di allarme.
- **Errori**: verranno registrati errori quali "Errore durante il download del file" ed errori critici.
- **Critico**: registra solo gli errori critici (errore che avvia la protezione antivirus).

Periodo: definire l'intervallo di tempo rispetto al quale si desiderano visualizzare i risultati.

- **Non specificato** (impostazione predefinita): la ricerca non viene eseguita nel periodo indicato ma nell'intero rapporto.
- **Ultimo giorno**
- **Ultima settimana**
- **Ultimo mese**
- **Periodo di tempo**: è possibile specificare il periodo di tempo esatto (data e ora) per ricercare esclusivamente i record appartenenti a uno specifico periodo di tempo.

Solo parole intere: trova solo i record contenenti una stringa corrispondente alla parola intera nella casella di testo **Cosa**.

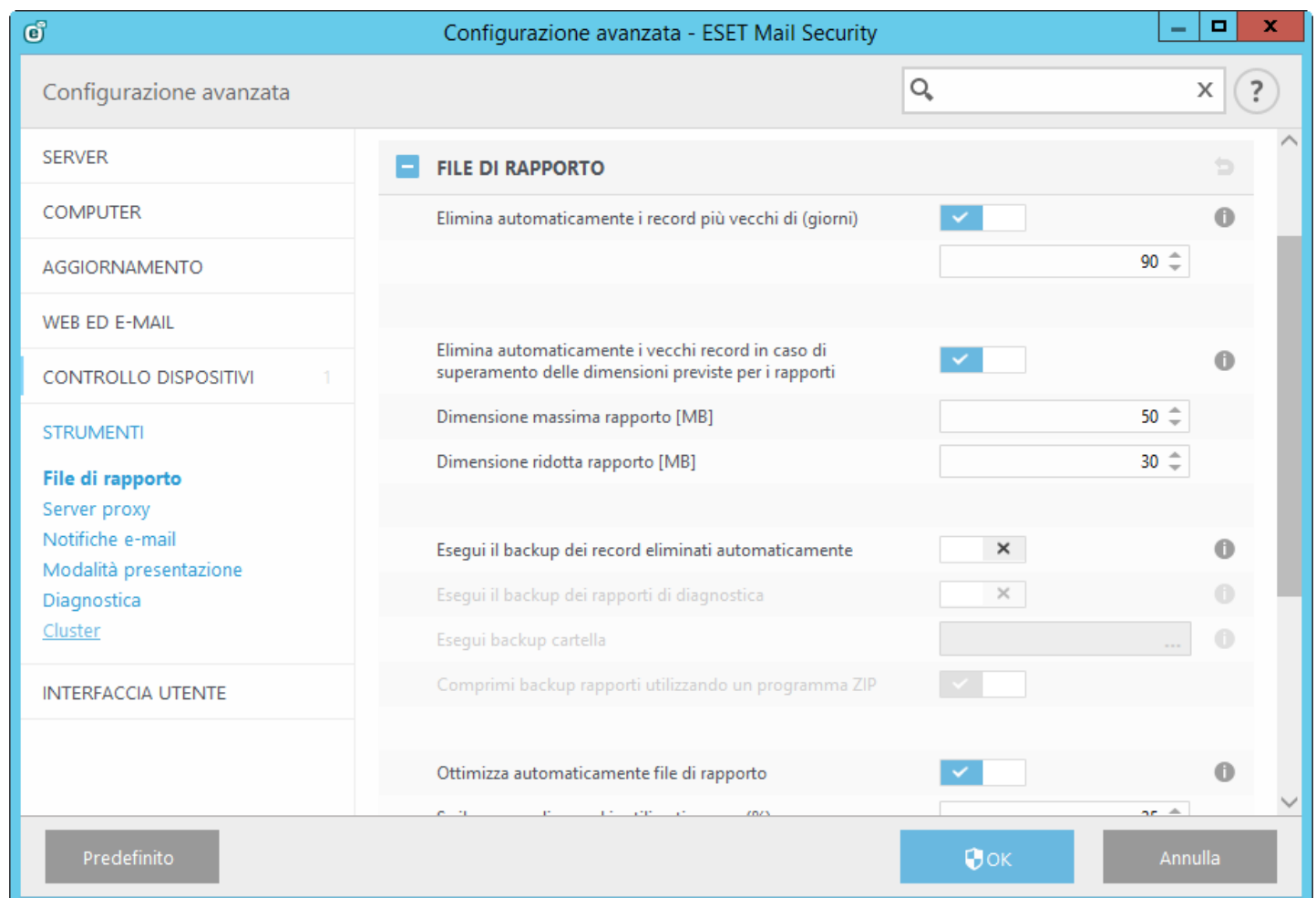
Maiuscole/minuscole: trova solo i record contenenti una stringa corrispondente al formato maiuscolo/minuscolo nella casella di testo **Cosa**.

Cerca verso l'alto: la ricerca viene eseguita dalla posizione corrente verso l'alto.

Dopo aver configurato le opzioni di ricerca, fare clic su **Trova** per iniziare la ricerca. La ricerca si interrompe quando viene trovato il primo record corrispondente. Fare nuovamente clic su **Trova** per visualizzare altri record. La ricerca nei file di rapporto viene eseguita dall'alto verso il basso, partendo dalla posizione corrente, ovvero dal record evidenziato.

5.6.6.3 Manutenzione rapporto

La configurazione della registrazione di ESET Mail Security è accessibile dalla finestra principale del programma.

Fare clic su **Configurazione** > **Configurazione avanzata** > **Strumenti** > **File di rapporto**. La sezione relativa ai rapporti viene utilizzata per definire come verranno gestiti. Il programma elimina automaticamente i rapporti meno recenti per liberare spazio sull'unità disco rigido.

- **Elimina record automaticamente**: le voci del rapporto più vecchie del numero di giorni specificato verranno

eliminate automaticamente.

- **Ottimizza automaticamente file di rapporto**: consente la deframmentazione automatica dei file di rapporto se si supera la percentuale specificata di record inutilizzati
- **Livello minimo di dettaglio del rapporto**: consente di specificare il livello minimo di dettaglio del rapporto. Opzioni disponibili:
  - **Record di diagnostica**: registra le informazioni necessarie per ottimizzare il programma e tutti i record precedenti
  - **Record informativi**: registra messaggi informativi che includono gli aggiornamenti riusciti e tutti i record indicati in precedenza
  - **Allarmi**: registra errori critici e messaggi di allarme
  - **Errori**: verranno registrati solo messaggi quali "Errore durante il download del file" ed errori critici
  - **Allarmi critici**: registra solo gli errori critici (errore che avvia la protezione antivirus e così via)

5.6.7 Server proxy

Nelle reti LAN di grandi dimensioni, la connessione del computer dell'utente a Internet può essere mediata da un server proxy. In questo caso, occorre definire le impostazioni seguenti. In caso contrario, il programma non sarà in grado di aggiornarsi automaticamente. In ESET Mail Security, il server proxy può essere configurato in due sezioni differenti della struttura Configurazione avanzata.

Le impostazioni del server proxy possono innanzitutto essere configurate in **Configurazione avanzata** da **Strumenti** > **Server proxy**. Specificando il server proxy a questo livello, si definiscono le impostazioni globali del server proxy per l'intera applicazione ESET Mail Security. Questi parametri vengono utilizzati da tutti i moduli che richiedono una connessione a Internet.

Per specificare le impostazioni del server proxy per questo livello, attivare il pulsante **Usa server proxy**, quindi inserire l'indirizzo del server proxy nel campo **Server proxy**, insieme al relativo numero di **Porta**.

Se la comunicazione con il server proxy richiede l'autenticazione, attivare il pulsante **Il server proxy richiede l'autenticazione** e inserire un **Nome utente** e una **Password** validi nei rispettivi campi. Fare clic su **Rileva** per rilevare e inserire automaticamente le impostazioni del server proxy. Verranno copiati i parametri specificati in Internet Explorer.

i **NOTA:** questa funzione non consente di recuperare i dati sull'autenticazione (nome utente e password). Tali informazioni devono quindi essere immesse dall'utente.

Le impostazioni del server proxy possono anche essere definite nella finestra Configurazione aggiornamento avanzata (**Configurazione avanzata** > **Aggiorna** > **Proxy HTTP** selezionando **Connessione tramite un server proxy** dal menu a discesa **Modalità proxy**). Questa impostazione è applicabile al profilo di aggiornamento fornito ed è consigliata sui notebook che ricevono spesso aggiornamenti delle firme antivirali da diverse postazioni. Per ulteriori informazioni su questa impostazione, consultare la sezione Configurazione aggiornamento avanzata.

5.6.8 Notifiche e-mail

ESET Mail Security invia automaticamente e-mail di notifica nel caso in cui si verifichi un evento con il livello di dettaglio selezionato. Attivare **Invia notifiche di eventi via e-mail** per attivare le notifiche e-mail.

NOTA: ESET Mail Security supporta i server SMTP con crittografia TLS.

- **Server SMTP**: server SMTP utilizzato per l'invio delle notifiche.
- **Nome utente e password**: se il server SMTP richiede l'autenticazione, questi campi devono essere compilati con nome utente e password validi per l'accesso al server SMTP.

- **Indirizzo mittente**: questo campo specifica l'indirizzo del mittente che verrà visualizzato nell'intestazione delle e-mail di notifica.
- **Indirizzo destinatario**: questo campo specifica l'indirizzo del destinatario che verrà visualizzato nell'intestazione delle e-mail di notifica.

- **Livello di dettaglio minimo per le notifiche**: specifica il livello di dettaglio minimo delle notifiche da inviare.
- **Attiva TLS**: attiva messaggi di avviso e notifiche supportati dalla crittografia TLS.

- **Intervallo in seguito al quale verranno inviate nuove e-mail di notifica (min.)**: intervallo in minuti in seguito al quale verrà inviata una nuova notifica tramite e-mail. Impostare il valore su 0 se si desidera inviare immediatamente queste notifiche.
- **Invia ciascuna notifica in un'e-mail separata**: attivando questa opzione, il destinatario riceverà una nuova e-mail per ogni singola notifica. Tale operazione potrebbe determinare la ricezione di un numero elevato di e-mail in un periodo di tempo ridotto.

Formato del messaggio

- **Formato dei messaggi di evento** : formato dei messaggi di evento che vengono visualizzati sui computer remoti. Consultare anche il paragrafo Modifica formato.
- **Formato dei messaggi di avviso per le minacce** : i messaggi di avviso e notifica delle minacce presentano un

formato predefinito. Si consiglia di non modificare questo formato. Tuttavia, in alcuni casi (ad esempio, se si dispone di un sistema di elaborazione delle e-mail automatizzato) potrebbe essere necessario modificare il formato dei messaggi. Consultare anche il paragrafo Modifica formato.

- **Utilizza caratteri alfabetici locali**: converte un messaggio e-mail nella codifica dei caratteri ANSI in base alle impostazioni della lingua di Windows (ad esempio, windows-1250). Se si lascia deselezionata questa opzione, il messaggio verrà convertito e codificato in ACSII a 7 bit (ad esempio, "á" verrà modificata in "a" e un simbolo sconosciuto verrà modificato in "?").
- **Utilizza codifica caratteri locali**: l'origine del messaggio e-mail verrà codificata in formato QP (Quoted-printable) che utilizza i caratteri ASCII ed è in grado di trasmettere correttamente speciali caratteri nazionali tramite e-mail nel formato a 8-bit (áéíóú).

5.6.8.1 Formato del messaggio

Le comunicazioni tra il programma e un utente remoto o un amministratore di sistema avvengono tramite e-mail o messaggi LAN (utilizzando il servizio Messenger di Windows®). Il formato predefinito dei messaggi e delle notifiche di avviso è adatto alla maggior parte delle situazioni. In alcune circostanze, potrebbe essere necessario modificare il formato dei messaggi di evento.

Nel messaggio, le parole chiave (stringhe separate dai segni %) vengono sostituite dalle informazioni effettive specificate. Sono disponibili le parole chiave seguenti:

- **%TimeStamp%**: data e ora dell'evento
- **%Scanner%**: modulo interessato
- **%ComputerName%**: nome del computer in cui si è verificato l'avviso
- **%ProgramName%**: programma che ha generato l'avviso
- **%InfectedObject%**: nome del file, del messaggio, ecc. infetto
- **%VirusName%**: identificazione dell'infezione
- **%ErrorDescription%**: descrizione di un evento non virale

Le parole chiave **%InfectedObject%** e **%VirusName%** vengono utilizzate solo nei messaggi di allarme delle minacce, mentre **%ErrorDescription%** viene utilizzata solo nei messaggi di evento.

5.6.9 Modalità presentazione

La modalità presentazione è una funzionalità pensata per gli utenti che richiedono un utilizzo ininterrotto del software, non desiderano essere disturbati dalle finestre popup e desiderano ridurre al minimo l'utilizzo della CPU. La modalità presentazione può essere utilizzata anche durante le presentazioni che non possono essere interrotte dall'attività antivirus. Se attivata, tutte le finestre popup verranno disattivate e le attività pianificate non verranno eseguite. La protezione del sistema è ancora in esecuzione in background, ma non richiede l'interazione dell'utente.

Fare clic su **Configurazione** > **Computer**, quindi sul pulsante accanto a **Modalità presentazione** per attivare la modalità presentazione manualmente. In **Configurazione avanzata** (F5), fare clic su **Strumenti** > **Modalità presentazione**, quindi sul pulsante accanto a **Attiva automaticamente modalità Presentazione quando vengono eseguite applicazioni in modalità a schermo intero** per far sì che la funzione ESET Mail Security attivi automaticamente la modalità presentazione quando vengono eseguite applicazioni in modalità a schermo intero. L'attivazione della modalità presentazione rappresenta un potenziale rischio per la protezione. Per tale motivo, l'icona relativa allo stato della protezione sulla barra delle attività diventa di colore arancione e viene visualizzato un avviso. Questo avviso verrà visualizzato anche nella finestra principale del programma dove **Modalità presentazione attivata** comparirà in arancione.

Dopo aver attivato **Attiva automaticamente modalità presentazione quando vengono eseguite applicazioni in modalità a schermo intero**, la modalità presentazione si attiverà all'avvio di un'applicazione in modalità a schermo intero e si interromperà automaticamente all'uscita dall'applicazione. Questa funzionalità si rivela particolarmente utile per l'attivazione della modalità presentazione subito dopo l'avvio di un gioco, l'apertura di un'applicazione in modalità a schermo intero o l'avvio di una presentazione.

È inoltre possibile selezionare **Disattiva automaticamente modalità presentazione** per definire l'intervallo di tempo espresso in minuti dopo il quale la modalità presentazione verrà automaticamente disattivata.

5.6.10 Diagnostica

La diagnostica fornisce dump sulle interruzioni delle applicazioni correlate ai processi ESET (ad esempio, *ekrn*). In caso di interruzione di un'applicazione, verrà generato un dump, che aiuta gli sviluppatori a eseguire il debug e correggere vari problemi di ESET Mail Security. Fare clic sul menu a discesa accanto a **Tipo di dump** e selezionare una delle tre opzioni disponibili:

- Selezionare **Disattiva** (impostazione predefinita) per disattivare questa funzionalità.
- **Mini**: registra il minor numero di informazioni utili che potrebbero contribuire all'identificazione del motivo alla base dell'arresto inaspettato dell'applicazione. Questo tipo di file dump risulta utile in caso di limitazioni di spazio. A causa delle informazioni limitate incluse, gli errori che non sono stati causati direttamente dalla minaccia in esecuzione quando si è verificato il problema potrebbero tuttavia non essere rilevati a seguito di un'analisi del file in questione.
- **Completo**: registra tutti i contenuti della memoria di sistema quando l'applicazione viene interrotta inaspettatamente. Un dump di memoria completo può contenere dati estrapolati dai processi in esecuzione al momento del recupero.

Directory di destinazione: directory nella quale verrà generato il dump durante l'arresto imprevisto.

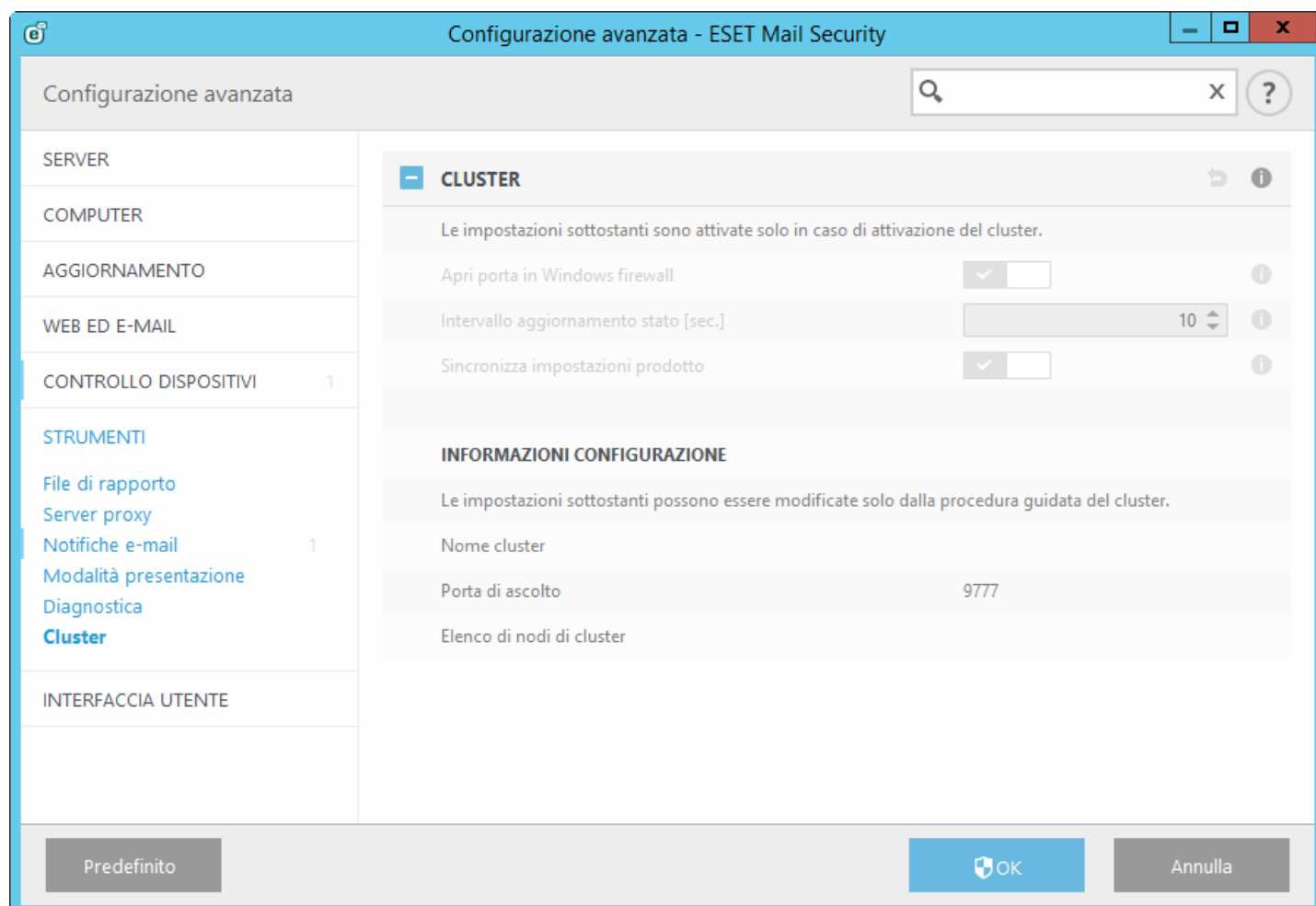
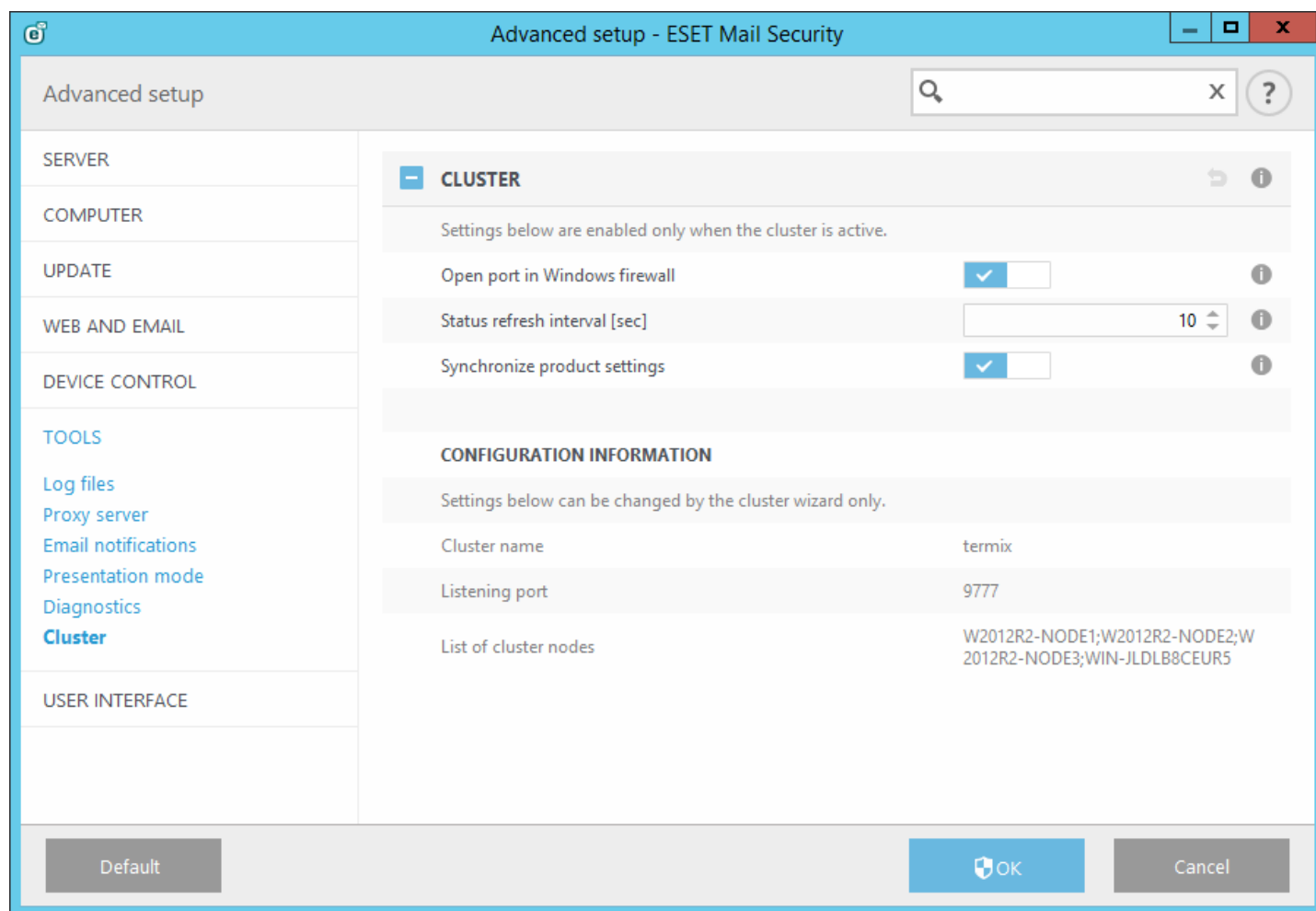
Apri cartella diagnostica: fare clic su **Apri** per aprire questa directory in una nuova finestra di *Windows Explorer*.

5.6.11 Supporto tecnico

Invia dati configurazione sistema: selezionare **Invia sempre** dal menu a discesa oppure **Chiedi prima di inviare** che comparirà prima dell'invio dei dati.

5.6.12 Cluster

Quando ESET Cluster è configurato, la funzione **Attiva cluster** è attiva automaticamente. È possibile disattivarla manualmente nella finestra Configurazione avanzata facendo clic sull'icona del pulsante. Tale operazione è idonea quando è necessario modificare la configurazione senza influenzare altri nodi in ESET Cluster. Questo pulsante consente solo di attivare o disattivare le funzionalità di ESET Cluster. Per configurare o eliminare correttamente il cluster, è necessario utilizzare la Procedura guidata cluster o Elimina cluster disponibile nella sezione **Strumenti** > **Cluster** della finestra principale del programma.

ESET Cluster non configurato e disattivato:

ESET Cluster correttamente configurato con relativi dettagli e opzioni:

Per ulteriori informazioni su ESET Cluster, fare clic qui.

5.7 Interfaccia utente

La sezione **Interfaccia utente** consente di configurare il comportamento dell'interfaccia utente grafica (GUI) del programma. È possibile modificare l'aspetto e gli effetti visivi del programma.

Per offrire un livello massimo di protezione, è possibile impedire eventuali modifiche non autorizzate del software mediante l'utilizzo dello strumento Configurazione dell'accesso.

Configurando la sezione Avvisi e notifiche, è possibile modificare il comportamento degli avvisi sulle minacce rilevate e le notifiche di sistema in modo da adattarli alle proprie esigenze.

Se si sceglie di non visualizzare alcune notifiche, queste verranno visualizzate nell'area Messaggi e stati disattivati. In tali finestre è possibile verificarne lo stato, visualizzare ulteriori dettagli oppure rimuoverle.

L'Integrazione menu contestuale verrà visualizzata facendo clic con il pulsante destro del mouse sull'oggetto selezionato. Utilizzare questo strumento per integrare gli elementi di controllo di ESET Mail Security nel menu contestuale.

La modalità presentazione è utile per gli utenti che desiderano utilizzare un'applicazione senza essere interrotti dalle finestre popup, dalle attività pianificate e da qualsiasi componente che potrebbe influire negativamente sulle risorse di sistema.

Elementi dell'interfaccia utente

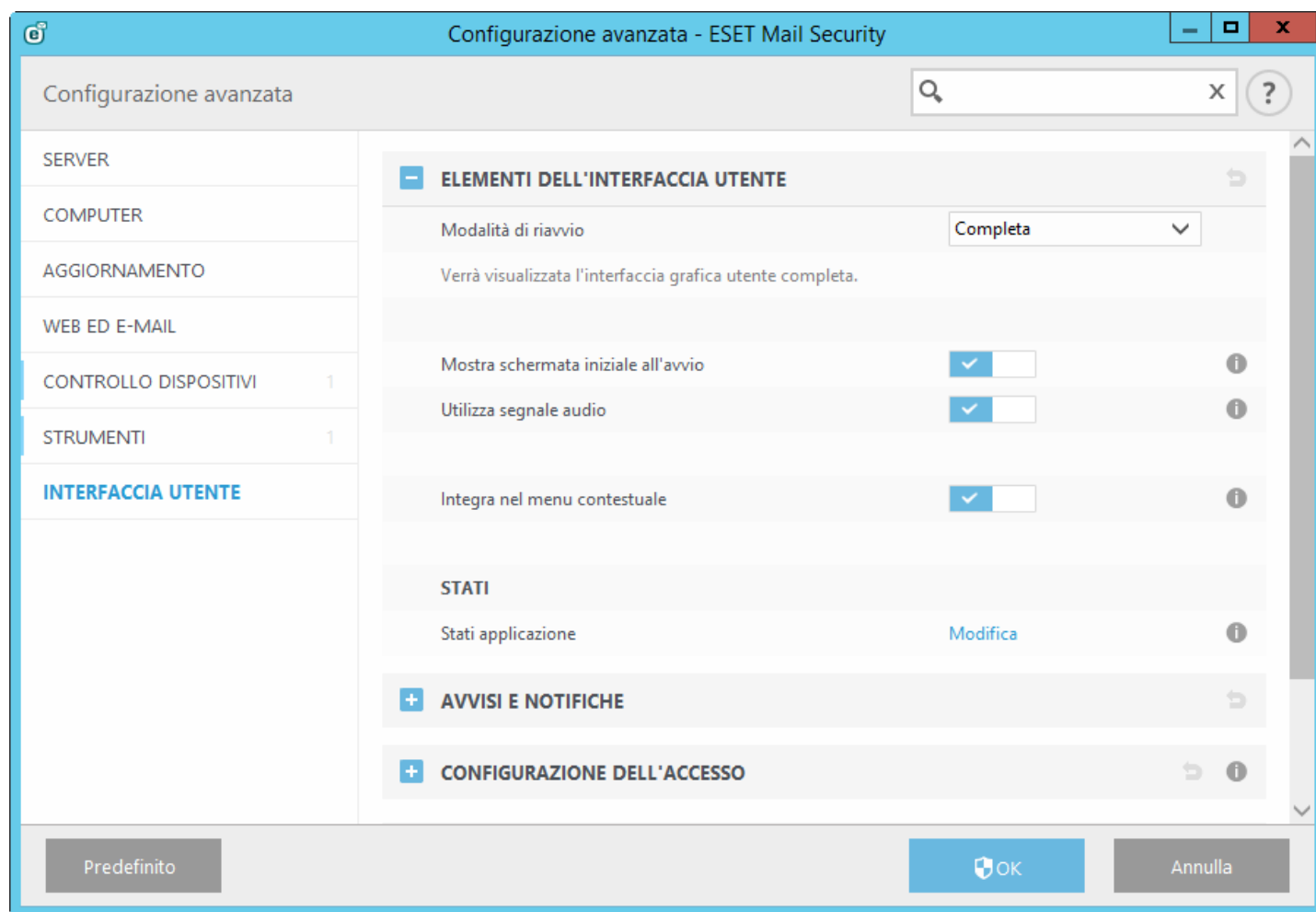
Le opzioni di configurazione dell'interfaccia utente in ESET Mail Security consentono di modificare l'ambiente di lavoro per adattarlo alle specifiche esigenze dell'utente. Queste opzioni di configurazione sono accessibili nel ramo **Interfaccia utente** > **Elementi dell'interfaccia utente** della struttura Configurazione avanzata di ESET Mail Security.

Nella sezione **Elementi dell'interfaccia utente** è possibile modificare l'ambiente di lavoro. L'interfaccia utente deve essere impostata su **Terminal** qualora gli elementi grafici rallentino le prestazioni del computer o causino altri problemi. L'utente potrebbe anche decidere di disattivare l'interfaccia utente grafica su un Terminal server. Per ulteriori informazioni su ESET Mail Security installato su Terminal server, consultare l'argomento Disattiva l'interfaccia utente grafica su Terminal Server.

Fare clic sul menu a discesa **Modalità di avvio GUI** per selezionare una delle seguenti modalità di avvio della (GUI):
Completa: verrà visualizzata l'interfaccia utente completa.
Terminal: non verranno visualizzati avvisi o notifiche. L'interfaccia utente grafica può essere avviata solo dall'amministratore.

Se si desidera disattivare la schermata iniziale di ESET Mail Security, deselezionare **Mostra schermata iniziale all'avvio**.

Per far sì che ESET Mail Security emetta un suono al verificarsi di eventi importanti durante un controllo, ad esempio in caso di rilevamento di una minaccia o al termine del controllo, selezionare **Utilizza segnale audio**.

Integra nel menu contestuale: integra gli elementi di controllo di ESET Mail Security nel menu contestuale.

Stati: fare clic su **Modifica** per gestire (attivare o disattivare) gli stati visualizzati nel riquadro Monitoraggio nel menu principale.

Stati applicazione: consente all'utente di attivare o disattivare lo stato di visualizzazione nel riquadro **Stato di protezione** nel menu principale.

5.7.1 Avvisi e notifiche

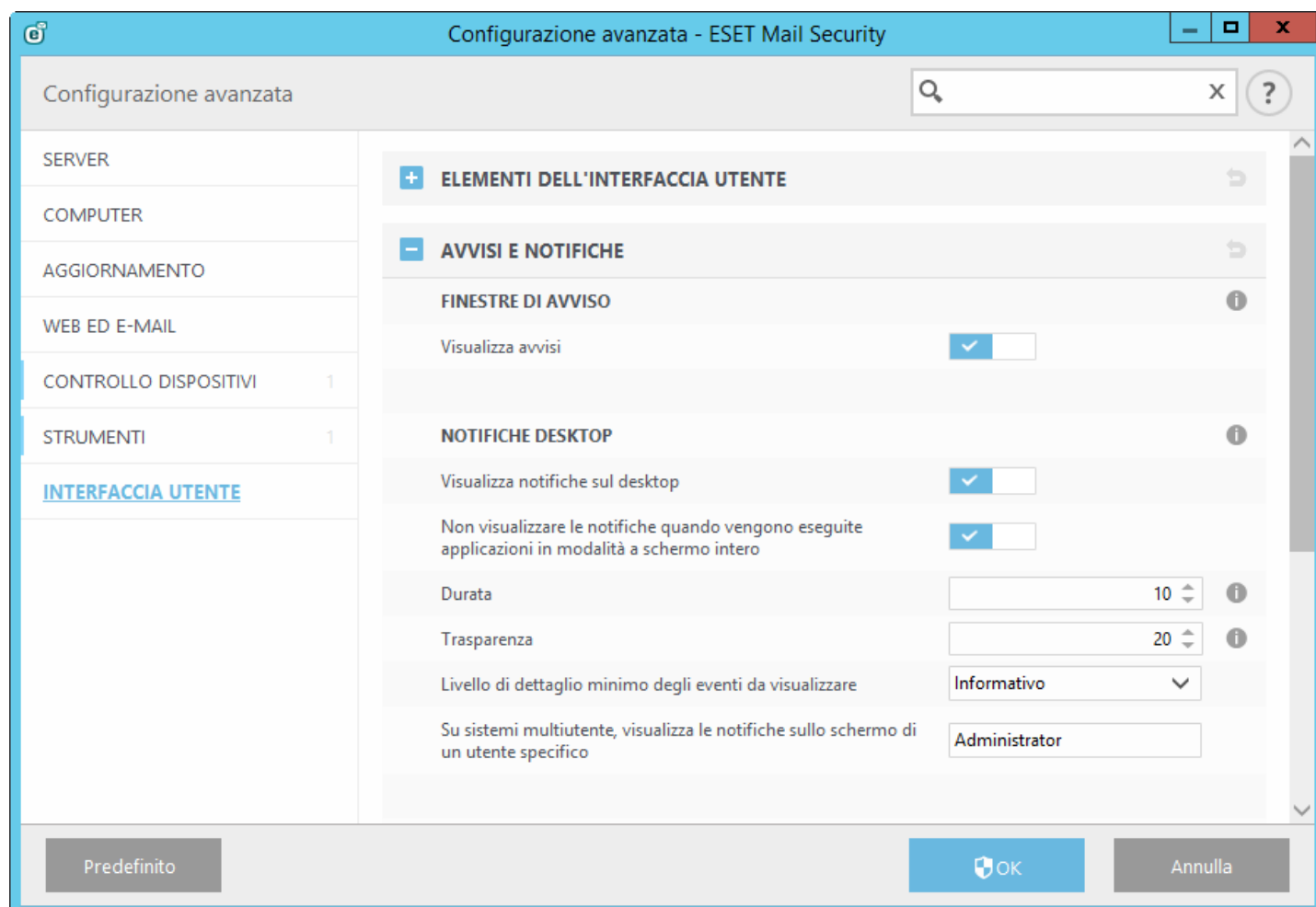
La sezione **Avvisi e notifiche** nell'**Interfaccia utente** consente di configurare la gestione dei messaggi di avviso e delle notifiche di sistema (ad esempio messaggi di aggiornamenti riusciti) in ESET Mail Security. È inoltre possibile impostare l'ora di visualizzazione e il livello di trasparenza delle notifiche sulla barra delle applicazioni del sistema (applicabile solo ai sistemi che supportano le notifiche sulla barra delle applicazioni).

Finestre di avviso

Disattivando **Visualizza avvisi**, tutte le finestre di avviso verranno annullate. Per tale motivo, è consigliabile eseguire tale operazione solo in un numero limitato di situazioni specifiche. Nella maggior parte dei casi, si consiglia di non modificare l'impostazione predefinita (opzione attivata).

Notifiche desktop

Le notifiche visualizzate sul desktop e i suggerimenti sono forniti esclusivamente a titolo informativo e non richiedono l'interazione dell'utente. Vengono visualizzate nell'area di notifica posta nell'angolo in basso a destra della schermata. Per attivare la visualizzazione delle notifiche sul desktop, selezionare **Visualizza notifiche sul desktop**. È possibile modificare opzioni più dettagliate, ad esempio l'orario di visualizzazione della notifica e la trasparenza della finestra seguendo le istruzioni fornite di seguito.

Attivare il pulsante **Non visualizzare le notifiche quando vengono eseguite applicazioni in modalità a schermo intero** per eliminare tutte le notifiche non interattive.

Finestre di messaggio

Per chiudere automaticamente le finestre popup dopo un determinato periodo di tempo, selezionare **Chiudi automaticamente le finestre di messaggio**. Se non vengono chiuse manualmente, le finestre di avviso vengono chiuse automaticamente una volta trascorso il periodo di tempo specificato.

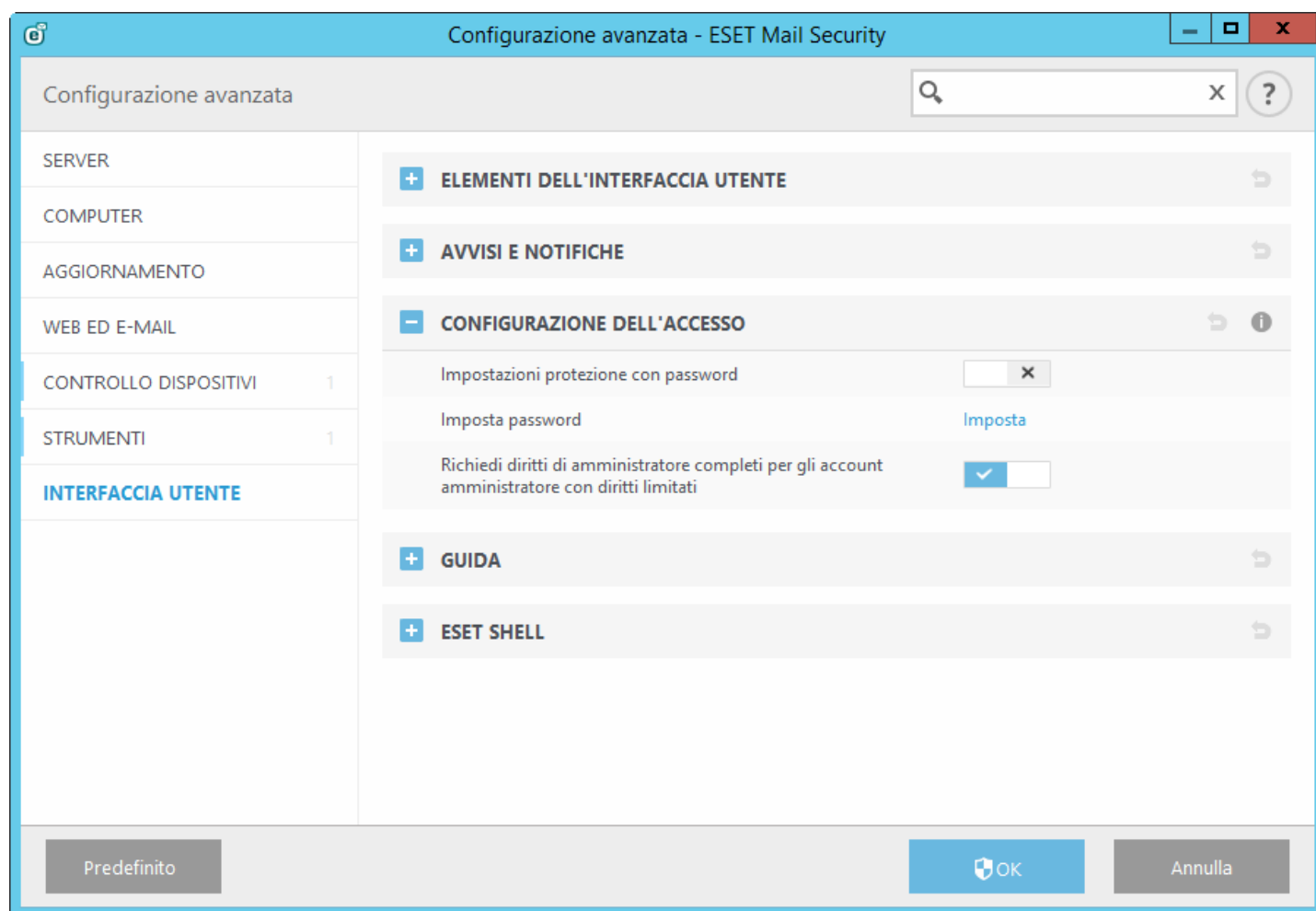
Il menu a discesa **Livello di dettaglio minimo degli eventi da visualizzare** consente all'utente di selezionare il livello

di gravità degli avvisi e delle notifiche da visualizzare. Sono disponibili le seguenti opzioni:

- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativo**: registra i messaggi informativi, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Allarmi**: registra errori critici e messaggi di allarme.
- **Errori**: verranno registrati errori quali "Errore durante il download del file" ed errori critici.
- **Critico**: registra solo gli errori critici (errore che avvia la protezione antivirus e così via).

L'ultima funzione in questa sezione consente di configurare la destinazione delle notifiche in un ambiente multi-utente. Nel campo **In sistemi multiutente, visualizza le notifiche sullo schermo di questo utente** viene specificato l'utente che riceverà le notifiche di sistema e di altro tipo sui sistemi che consentono la connessione simultanea di più utenti. In genere si tratta di un amministratore di sistema o di rete. Questa opzione è utile soprattutto per i server di terminali, a condizione che tutte le notifiche di sistema vengano inviate all'amministratore.

5.7.2 Configurazione dell'accesso

Per garantire un livello di protezione massimo del sistema, è fondamentale che ESET Mail Security sia configurato correttamente. Qualsiasi modifica non appropriata potrebbe causare la perdita di dati importanti. Per evitare modifiche non autorizzate, i parametri di configurazione di ESET Mail Security possono essere protetti con password. Le impostazioni di configurazione per la protezione con password sono disponibili nel sottomenu **Configurazione dell'accesso** sotto a **Interfaccia utente** nella struttura Configurazione avanzata.

Proteggi impostazioni con password: blocca/sblocca i parametri di impostazione del programma. Fare clic per aprire la finestra di configurazione della password.

Per impostare o modificare una password al fine di proteggere i parametri di configurazione, fare clic su **Imposta password**.

Richiedi diritti di amministratore completi per gli account con diritti limitati: selezionare questa opzione per

richiedere all'utente corrente (nel caso non disponga dei diritti di amministratore) di immettere nome utente e password per la modifica di alcuni parametri del sistema (analogo a Controllo dell'account utente in Windows Vista). Tali modifiche includono la disattivazione dei moduli di protezione.

5.7.2.1 Password

Per evitare modifiche non autorizzate, i parametri di impostazione di ESET Mail Security possono essere protetti con password.

5.7.2.2 Configurazione password

Per proteggere i parametri di configurazione di ESET Mail Security al fine di evitare una modifica non autorizzata, è necessario impostare una nuova password. Se si desidera modificare una password esistente, è necessario digitare la vecchia password nel campo **Vecchia password**, inserire la nuova nel campo **Nuova password**, selezionare **Conferma password** e fare clic su **OK**. La password verrà richiesta per apportare future modifiche a ESET Mail Security.

5.7.3 Guida

Premendo il tasto **F1** oppure facendo clic sul pulsante **?**, si aprirà la finestra di una guida on-line, che rappresenta il documento di supporto principale. È tuttavia disponibile anche una copia off-line che viene fornita in seguito all'installazione del programma. La guida off-line si apre, ad esempio, in caso di mancata disponibilità di una connessione a Internet.

L'ultima versione della guida on-line verrà visualizzata automaticamente in presenza di una connessione a Internet funzionante.

5.7.4 ESET Shell

Modificando l'impostazione del **Criterio di esecuzione ESET Shell** di eShell, è possibile configurare i diritti di accesso alle impostazioni, alle funzioni e ai dati del prodotto. L'impostazione predefinita è **Scripting limitato**. Tuttavia, se necessario, è possibile modificarla scegliendo tra **Disattivato**, **Di sola lettura** o **Accesso completo**.

- **Disattivato**: eShell non può essere assolutamente utilizzato. È consentita solo la configurazione di eShell stesso nel `contesto` ui eshell. È possibile personalizzare l'aspetto di eShell, ma non accedere alle impostazioni o ai dati del prodotto.
- **Di sola lettura**: eShell può essere utilizzato come strumento di monitoraggio. È possibile visualizzare tutte le impostazioni sia in modalità interattiva sia in modalità batch, ma non modificare le impostazioni, le funzioni o i dati.
- **Scripting limitato**: in modalità interattiva, è possibile visualizzare e modificare tutte le impostazioni, le funzioni e i dati. In modalità batch, eShell funzionerà come in modalità di sola lettura. Tuttavia, in caso di utilizzo di file batch firmati, l'utente potrà modificare le impostazioni e i dati.
- **Accesso completo**: accesso illimitato a tutte le impostazioni sia in modalità interattiva sia in modalità batch. È possibile visualizzare e modificare qualsiasi impostazione. Per eseguire eShell in modalità accesso completo, è necessario utilizzare un account amministratore. In caso di attivazione del Controllo dell'account utente (UAC), è richiesta anche l'elevazione.

5.7.5 Disattiva l'interfaccia utente grafica su Terminal Server

In questo capitolo viene illustrato come disattivare l'interfaccia utente di ESET Mail Security in esecuzione su Windows Terminal Server per le sessioni utente.

In genere l'interfaccia utente di ESET Mail Security viene avviata ogni volta che un utente remoto accede al server e crea una sessione terminal. Ciò non è di norma auspicabile sui Terminal Server. Per disattivare l'interfaccia utente grafica per le sessioni terminal, utilizzare eShell eseguendo `il comando` set `ui ui gui-start-mode terminal`. Questa operazione imposterà l'interfaccia utente grafica in modalità terminal. Le due modalità disponibili per l'avvio dell'interfaccia utente grafica sono:

```
set ui ui gui-start-mode full
set ui ui gui-start-mode terminal
```

Per scoprire la modalità attualmente in uso, eseguire il comando `get ui ui gui-start-mode`.

NOTA: in caso di installazione di ESET Mail Security su un server Citrix, si consiglia di utilizzare le impostazioni descritte in questo articolo della Knowledge Base.

5.7.6 Messaggi e stati disattivati

Messaggi di conferma: consente all'utente di visualizzare un elenco di messaggi di conferma che è possibile decidere di visualizzare o non visualizzare.

Stati applicazioni disattivate: consente all'utente di attivare o disattivare lo stato di visualizzazione nel riquadro **Stato di protezione** nel menu principale.

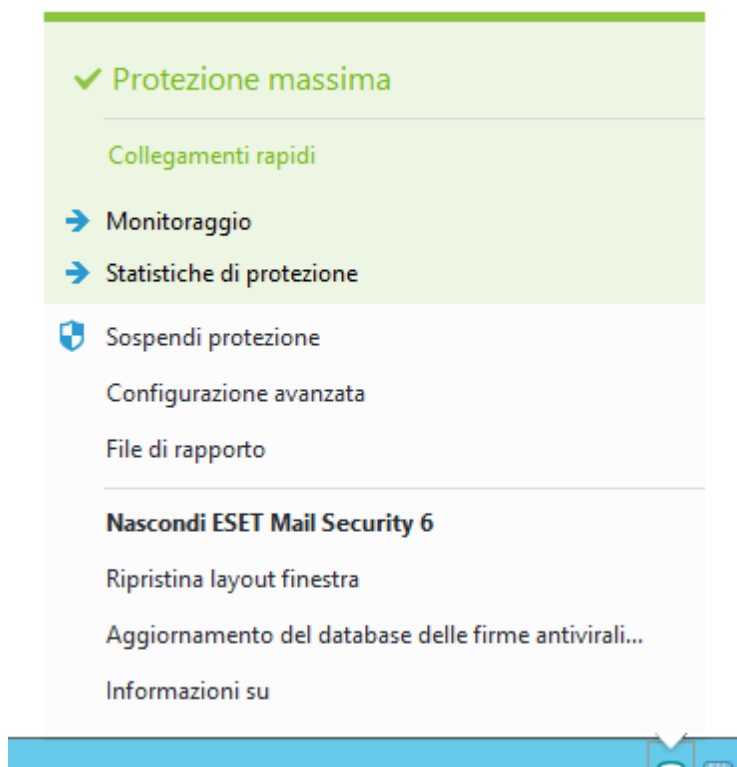
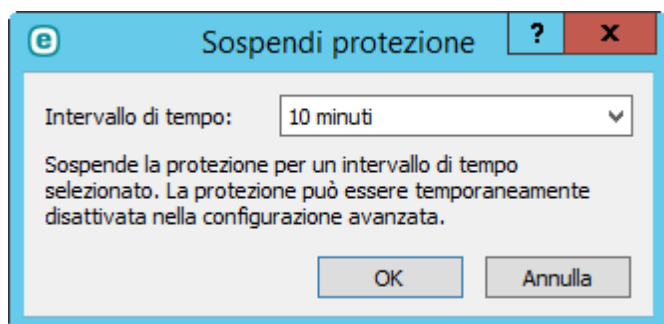
5.7.6.1 Messaggi di conferma

Questa finestra di dialogo consente di visualizzare messaggi di conferma in ESET Mail Security prima dell'esecuzione di qualsiasi azione. Selezionare o deselezionare la casella di controllo accanto a ciascun messaggio di conferma per consentirlo o disattivarlo.

5.7.6.2 Stati applicazioni disattivate

In questa finestra di dialogo è possibile selezionare o deselezionare gli stati delle applicazioni che verranno visualizzati e di quelli che non verranno visualizzati, durante, ad esempio, la sospensione della protezione antivirus e antispyware o quando si attiva la modalità presentazione. Verrà inoltre visualizzato uno stato dell'applicazione in caso di mancata attivazione del prodotto o di scadenza della licenza.

5.7.7 Icona della barra delle applicazioni

Alcune delle principali opzioni di configurazione e funzionalità sono disponibili facendo clic con il pulsante destro del mouse sull'icona della barra delle applicazioni .

Sospendi protezione: consente di visualizzare la finestra di dialogo di conferma per disattivare la Protezione antivirus e antispyware che protegge da attacchi controllando file e comunicazioni Web e e-mail.

Il menu a discesa **Intervallo di tempo** rappresenta l'intervallo di tempo durante il quale la Protezione antivirus e antispyware verrà disattivata.

Configurazione avanzata: selezionare questa opzione per accedere alla struttura **Configurazione avanzata**. È inoltre possibile accedere alla configurazione avanzata premendo il tasto F5 oppure accedendo a **Configurazione** > **Configurazione avanzata**.

File di rapporto: i File di rapporto contengono informazioni relative a tutti gli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate.

Nascondi ESET Mail Security: nasconde la finestra di ESET Mail Security dalla schermata.

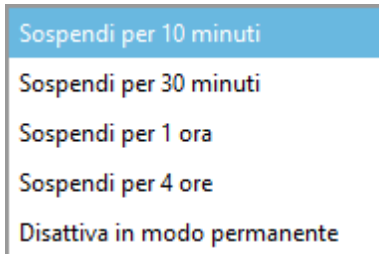
Ripristina layout finestra: ripristina le dimensioni predefinite e la posizione sullo schermo della finestra di ESET Mail Security.

Aggiornamento database firme antivirali: avvia l'aggiornamento del database delle firme antivirali per garantire il livello di protezione stabilito dall'utente contro codici dannosi.

Informazioni su: fornisce informazioni sul sistema, dettagli sulla versione installata di ESET Mail Security e sui relativi moduli dei programmi installati, nonché la data di scadenza della licenza. Le informazioni sul sistema

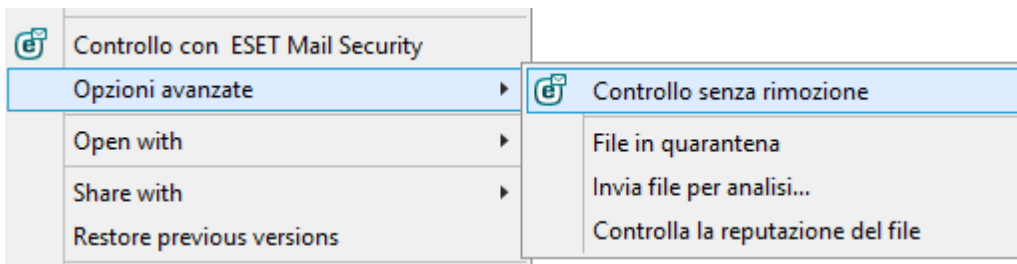
operativo e le risorse di sistema sono disponibili in fondo alla pagina.

5.7.7.1 Sospendi protezione

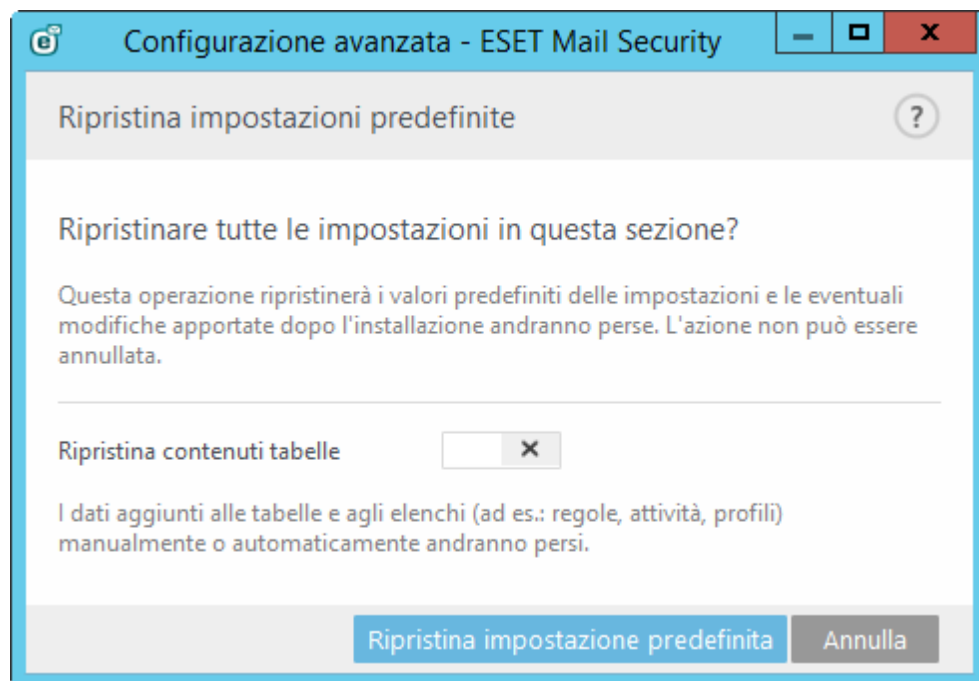
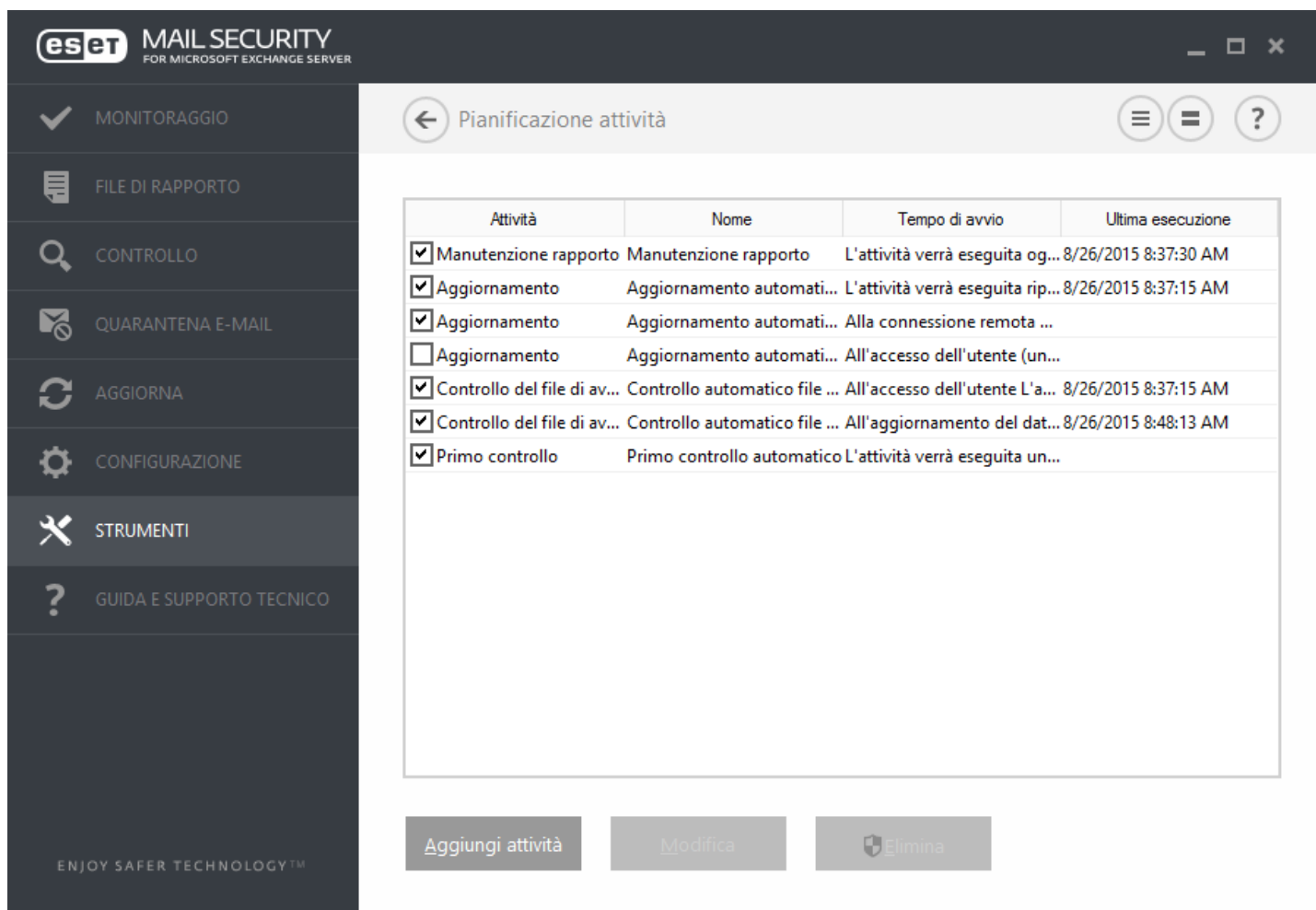
Tutte le volte che l'utente interrompe temporaneamente la protezione antivirus e antispyware utilizzando l'icona della barra delle applicazioni, comparirà la finestra di dialogo **Sospendi temporaneamente la protezione**. Tale operazione disattiverà la protezione da malware per il periodo di tempo selezionato (per disattivare la protezione in modo permanente, è necessario utilizzare la Configurazione avanzata). Utilizzare questa opzione con prudenza, in quanto la disattivazione della protezione espone il sistema alle minacce.

5.7.8 Menu contestuale

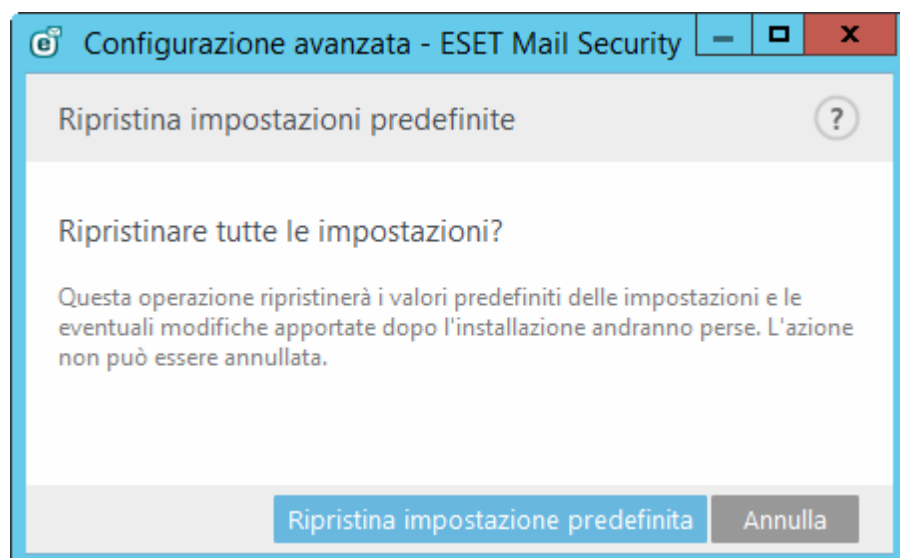
Il menu contestuale viene visualizzato facendo clic con il pulsante destro del mouse su un oggetto (file). Nel menu sono elencate tutte le azioni che è possibile eseguire su un oggetto.

Nel menu contestuale è possibile integrare gli elementi del controllo di ESET Mail Security. Le opzioni di configurazione per questa funzionalità sono disponibili nella struttura Configurazione avanzata sotto a **Interfaccia utente** > **Elementi dell'interfaccia utente**.

Integra nel menu contestuale: integra gli elementi di controllo di ESET Mail Security nel menu contestuale.

5.8 Ripristina tutte le impostazioni in questa sezione

Ripristina le impostazioni predefinite del modulo impostate da ESET. Si tenga presente che le eventuali modifiche apportate andranno perse facendo clic su **Ripristina impostazione predefinita**.

Ripristina contenuti tabelle: attivando questa opzione, le regole, le attività o i profili aggiunti manualmente o automaticamente andranno persi.

5.9 Ripristina impostazioni predefinite

Lo stato di tutte le impostazioni dei moduli del programma verrà ripristinato sui valori originali come dopo una nuova installazione.

5.10 Pianificazione attività

È possibile accedere a **Pianificazione attività** nel menu principale di ESET Mail Security in **Strumenti**. La Pianificazione attività contiene un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, ad esempio data, ora e profilo di controllo predefiniti utilizzati.

Per impostazione predefinita, in **Pianificazione attività** vengono visualizzate le attività pianificate seguenti:

- **Manutenzione rapporto**
- **Aggiornamento automatico periodico**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**
- **Controllo automatico file di avvio (dopo l'accesso utente)**
- **Controllo automatico file di avvio (dopo il completamento dell'aggiornamento del database delle firme antivirali)**
- **Primo controllo automatico**

Per modificare la configurazione di un'attività pianificata esistente (predefinita o definita dall'utente), fare clic con il pulsante destro del mouse sull'attività e selezionare **Modifica...** oppure selezionare l'attività che si desidera modificare e fare clic sul pulsante **Modifica...**.

5.10.1 Dettagli attività

Inserire il nome dell'attività e selezionare una delle opzioni relative al **Tipo di attività**, quindi fare clic su **Avanti**:

- **Esegui applicazione esterna**
- **Manutenzione rapporto**
- **Controllo del file di avvio del sistema**
- **Crea uno snapshot dello stato del computer**
- **Controllo del computer su richiesta**
- **Primo controllo**
- **Aggiornamento**

Esecuzione attività: l'attività specificata verrà eseguita solo una volta alla data e all'ora indicate.

Un'attività può essere ignorata se il computer è alimentato dalla batteria o è spento. Selezionare una di queste opzioni relative all'attività e fare clic su **Avanti**:

- Al prossimo orario pianificato
- Prima possibile
- Immediatamente, se l'ora dall'ultima esecuzione supera un valore specificato (ore)

5.10.2 Tempo attività: una volta

Esecuzione attività: l'attività specificata verrà eseguita solo una volta alla data e all'ora indicate.

5.10.3 Tempo attività

L'attività verrà eseguita ripetutamente in base all'intervallo temporale specificato. Selezionare una delle seguenti opzioni temporali:

- **Una volta**: l'attività verrà eseguita solo una volta, alla data e all'ora predefinite.
- **Ripetutamente**: l'attività verrà eseguita in base all'intervallo specificato (in ore).
- **Ogni giorno**: l'attività verrà eseguita ogni giorno all'ora specificata.
- **Ogni settimana**: l'attività verrà eseguita una o più volte alla settimana, nei giorni e nelle ore specificati.
- **Quando si verifica un evento**: l'attività verrà eseguita quando si verifica un evento specifico.

Ignora attività se in esecuzione su un computer alimentato dalla batteria: un'attività non verrà eseguita al momento del lancio se il computer in uso è alimentato dalla batteria. Questa regola vale anche per i computer alimentati da gruppi di continuità.

5.10.4 Tempo attività: ogni giorno

L'attività verrà eseguita periodicamente ogni giorno all'ora specificata.

5.10.5 Tempo attività: ogni settimana

L'attività verrà eseguita ogni settimana nel giorno e nell'ora selezionati.

5.10.6 Tempo attività: quando si verifica un evento

L'attività viene avviata da uno degli eventi seguenti:

- **A ogni avvio del computer**
- **Al primo avvio del computer ogni giorno**
- **Connessione remota a Internet/VPN**
- **Aggiornamento del database delle firme antivirali completato**
- **Aggiornamento dei componenti di programma completato**
- **Accesso utente**
- **Rilevamento delle minacce**

Quando si pianifica un'attività avviata da un evento, è possibile specificare l'intervallo minimo tra il completamento

di un'attività e l'altra. Se si esegue ad esempio l'accesso al computer più volte al giorno, scegliere 24 ore per eseguire l'attività solo al primo accesso del giorno, quindi il giorno successivo.

5.10.7 Dettagli attività: esegui applicazione

Questa scheda consente di pianificare l'esecuzione di un'applicazione esterna.

- **File eseguibile**: scegliere un file eseguibile dalla struttura della directory, fare clic sull'opzione **...** oppure immettere manualmente il percorso.
- **Cartella di lavoro**: specificare la directory di lavoro dell'applicazione esterna. Tutti i file temporanei del **File eseguibile** selezionato verranno creati all'interno di questa directory.
- **Parametri**: parametri della riga di comando per l'applicazione (facoltativo).

Fare clic su **Fine** per confermare l'attività.

5.10.8 Attività ignorata

Se l'attività non è stata eseguita all'ora predefinita, è possibile specificare il momento in cui dovrà essere eseguita:

- **Al prossimo orario pianificato**: l'attività verrà eseguita all'ora specificata (ad esempio, dopo 24 ore).
- **Prima possibile**: l'attività verrà eseguita il prima possibile, quando le azioni che ne impediscono l'esecuzione non saranno più valide.
- **Immediatamente, se l'ora dall'ultima esecuzione supera un valore specificato** - **Ora dall'ultima esecuzione (ore)**: dopo aver selezionato questa opzione, l'attività verrà sempre ripetuta dopo il periodo di tempo (in ore) specificato.

5.10.9 Dettagli attività Pianificazione attività

Questa finestra di dialogo contiene informazioni dettagliate sull'attività pianificata selezionata, che è possibile visualizzare facendo doppio clic su un'attività personalizzata, quindi facendo clic con il pulsante destro del mouse su un'attività pianificata personalizzata e selezionando **Mostra dettagli attività**.

5.10.10 Aggiorna profili

Se si desidera aggiornare il programma da due server di aggiornamento, è necessario creare due profili di aggiornamento differenti. Se il primo non riesce a scaricare i file dell'aggiornamento, il programma passa automaticamente al secondo. Questa soluzione risulta utile, ad esempio, per i notebook, che generalmente vengono aggiornati da un server di aggiornamento LAN locale, sebbene i proprietari si connettano spesso a Internet utilizzando altre reti. In questo modo, se il primo profilo non riesce a completare l'operazione, il secondo esegue automaticamente il download dei file dai server di aggiornamento ESET.

Ulteriori informazioni sui profili di aggiornamento sono disponibili nel capitolo Aggiornamento.

5.10.11 Creazione di nuove attività

Per creare una nuova attività in Pianificazione attività, fare clic sul pulsante **Aggiungi attività** oppure fare clic con il tasto destro del mouse e selezionare **Aggiungi** dal menu contestuale. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione esterna**: consente di pianificare l'esecuzione di un'applicazione esterna.
- **Manutenzione rapporto**: file di rapporto contenenti elementi rimasti dai record eliminati. Questa attività ottimizza periodicamente i record nei file di rapporto allo scopo di garantire un funzionamento efficiente.
- **Controllo del file di avvio del sistema**: consente di controllare i file la cui esecuzione è consentita all'avvio del sistema o all'accesso.
- **Crea uno snapshot dello stato del computer**: crea uno snapshot del computer ESET SysInspector, raccoglie informazioni dettagliate sui componenti del sistema (ad esempio, driver e applicazioni) e valuta il livello di rischio di ciascun componente.
- **Controllo computer su richiesta**: consente di eseguire un controllo di file e di cartelle sul computer in uso.
- **Primo controllo**: per impostazione predefinita, 20 minuti dopo l'installazione o il riavvio, verrà eseguito un Controllo del computer come attività con priorità bassa.
- **Aggiorna**: pianifica un'attività di aggiornamento aggiornando il database delle firme antivirali e i moduli del programma.

Poiché **Aggiorna** rappresenta una delle attività pianificate utilizzata con maggiore frequenza, verranno illustrate le modalità in cui è possibile aggiungere una nuova attività di aggiornamento.

Inserire un nome per l'attività nel campo **Nome attività**. Dal menu a discesa **Tipo di attività**, selezionare **Aggiornamento** e fare clic su **Avanti**.
Premere il pulsante **Attivata** se si desidera attivare l'attività (è possibile eseguire questa operazione in un secondo momento selezionando/deselezionando la casella di controllo nell'elenco di attività pianificate), fare clic su **Avanti** e selezionare una delle opzioni relative alla frequenza di esecuzione:
Una volta, **Ripetutamente**, **Ogni giorno**, **Ogni settimana** e **Quando si verifica un evento**. In base alla frequenza selezionata, verrà richiesto di specificare i diversi parametri di aggiornamento. È quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le tre opzioni riportate di seguito:

- **Al prossimo orario pianificato**
- **Prima possibile**
- **Immediatamente, se l'ora dall'ultima esecuzione supera un valore specificato** (è possibile definire l'intervallo utilizzando la casella di scorrimento Ora dall'ultima esecuzione)

Nel passaggio successivo, viene visualizzata una finestra contenente un riepilogo delle informazioni sull'attività pianificata corrente. Fare clic su **Fine** una volta terminate le modifiche.

Verrà visualizzata una finestra di dialogo in cui è possibile scegliere i profili da utilizzare per l'attività pianificata. Qui è possibile impostare il profilo primario e alternativo. Il profilo alternativo viene utilizzato se l'attività non può essere completata mediante l'utilizzo del profilo primario. Confermare facendo clic su **Fine**. A questo punto, la nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate.

5.11 Quarantena

La funzione principale della quarantena è archiviare i file infetti in modo sicuro. I file devono essere messi in quarantena se non è possibile pulirli, se non è sicuro o consigliabile eliminarli o, infine, se vengono erroneamente rilevati come minacce da ESET Mail Security.

È possibile mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto ma non viene rilevato dallo scanner antivirus. I file messi in quarantena possono essere inviati al laboratorio antivirus ESET per l'analisi.

I file salvati nella cartella della quarantena possono essere visualizzati in una tabella contenente la data e l'ora della quarantena, il percorso originale del file infetto, la dimensione in byte, il motivo (ad esempio, oggetto aggiunto dall'utente) e il numero di minacce (ad esempio, se si tratta di un archivio contenente più infiltrazioni).

Mettere file in quarantena

ESET Mail Security mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto a disattivare questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti selezionando **Quarantena.** I file della quarantena verranno rimossi dalla loro posizione originale. Per questa operazione è possibile utilizzare anche il menu contestuale: fare clic con il pulsante destro del mouse sulla finestra **Quarantena** e selezionare **Quarantena**.

Ripristino dalla quarantena

È possibile ripristinare nella posizione di origine i file messi in quarantena. Per far ciò, utilizzare la funzione **Ripristina**, disponibile nel menu contestuale, facendo clic con il pulsante destro del mouse sul file desiderato nella finestra Quarantena. Se un file è contrassegnato come applicazione potenzialmente indesiderata, sarà disponibile l'opzione **Ripristina ed escludi dal controllo**. Per ulteriori informazioni su questo tipo di applicazione, consultare la relativa voce del glossario. Il menu contestuale contiene anche l'opzione **Ripristina in...**, che consente di ripristinare i file in una posizione diversa da quella di origine da cui sono stati eliminati.

ℹ **NOTA:** se il programma mette in quarantena per errore un file non dannoso, escludere il file dal controllo dopo averlo ripristinato e inviarlo al Supporto tecnico ESET.

Invio di un file dalla cartella Quarantena

Se un file sospetto che non è stato rilevato dal programma è stato messo in quarantena o se un file è stato segnalato erroneamente come infetto (ad esempio, mediante un'analisi euristica del codice) e quindi messo in quarantena, è necessario inviarlo al laboratorio antivirus ESET. Per inviare un file dalla cartella Quarantena, fare clic con il pulsante destro del mouse su di esso e selezionare **Invia per analisi** dal menu contestuale.

5.11.1 Mettere file in quarantena

ESET Mail Security mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto a disattivare questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti selezionando **Quarantena**. In tal caso, il file originale non viene rimosso dalla posizione di origine. Per questa operazione è possibile utilizzare anche il menu contestuale: fare clic con il pulsante destro del mouse sulla finestra **Quarantena** e selezionare **Quarantena**.

5.11.2 Ripristino dalla quarantena

È possibile ripristinare nella posizione di origine i file messi in quarantena. Per ripristinare un file messo in quarantena, fare clic con il pulsante destro del mouse nella finestra Quarantena e selezionare **Ripristina** dal menu contestuale. Se un file è contrassegnato come applicazione potenzialmente indesiderata, sarà disponibile anche l'opzione **Ripristina ed escludi dal controllo**. Il menu contestuale contiene anche l'opzione **Ripristina in...**, che consente di ripristinare un file in una posizione diversa da quella di origine da cui è stato eliminato.

Eliminazione dalla quarantena: fare clic con il pulsante destro del mouse su un oggetto specifico e selezionare **Elimina dalla quarantena** oppure selezionare l'oggetto che si desidera eliminare e premere **Elimina** sulla tastiera. È inoltre possibile selezionare vari oggetti ed eliminarli contemporaneamente.

ℹ **NOTA**: se il programma ha messo in quarantena per errore un file non dannoso, escludere il file dal controllo dopo averlo ripristinato e inviarlo al Supporto tecnico ESET.

5.11.3 Invio di file dalla quarantena

Se un file sospetto che non è stato rilevato dal programma è stato messo in quarantena, o se un file è stato valutato erroneamente come infetto (ad esempio, da un'analisi euristica del codice) e quindi messo in quarantena, inviarlo ai laboratori delle minacce ESET. Per inviare un file dalla cartella di quarantena, fare clic con il pulsante destro del mouse sul file e selezionare **Invia per analisi** dal menu contestuale.

5.12 Aggiornamenti del sistema operativo

Nella finestra Aggiornamenti del sistema è visualizzato un elenco di aggiornamenti disponibili per il download e l'installazione. Il livello di priorità è visualizzato accanto al nome dell'aggiornamento.

Fare clic su **Esegui aggiornamento di sistema** per avviare il download e l'installazione degli aggiornamenti del sistema operativo.

Fare clic con il pulsante destro del mouse su qualsiasi riga dell'aggiornamento, quindi selezionare **Visualizza informazioni** per visualizzare una finestra popup contenente informazioni aggiuntive.

6. Glossario

6.1 Tipi di infiltrazioni

Un'infiltrazione è una parte di software dannoso che tenta di entrare e/o danneggiare il computer di un utente.

6.1.1 Virus

Un virus è un'infiltrazione che danneggia i file esistenti sul computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro.

I virus attaccano principalmente i file eseguibili e i documenti. Per replicarsi, un virus allega se stesso all'interno di un file di destinazione. In breve, un virus funziona nel seguente modo: dopo l'esecuzione del file infetto, il virus si attiva (prima dell'applicazione originale) ed esegue la sua attività predefinita. L'applicazione originale viene eseguita solo dopo questa operazione. Un virus non può infettare un computer a meno che un utente (accidentalmente o deliberatamente) esegua o apra il programma dannoso.

I virus possono essere classificati in base agli scopi e ai diversi livelli di gravità. Alcuni di essi sono estremamente dannosi poiché sono in grado di eliminare deliberatamente i file da un disco rigido. Altri, invece, non causano veri e propri danni, poiché il loro scopo consiste esclusivamente nell'infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

È importante tenere presente che i virus (se paragonati a trojan o spyware) sono sempre più rari, poiché non sono commercialmente allettanti per gli autori di software dannosi. Inoltre, il termine "virus" è spesso utilizzato in modo errato per indicare tutti i tipi di infiltrazioni. Attualmente, l'utilizzo di questo termine è stato superato e sostituito dalla nuova e più accurata definizione di "malware" (software dannoso).

Se il computer in uso è infettato da un virus, è necessario ripristinare lo stato originale dei file infetti, ovvero pulirli utilizzando un programma antivirus.

Tra i virus più noti si segnalano: OneHalf, Tenga e Yankee Doodle.

6.1.2 Worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite una rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di replicarsi e di viaggiare autonomamente, in quanto non dipendono da file host (o settori di avvio). I worm si diffondono attraverso indirizzi e-mail all'interno della lista dei contatti degli utenti oppure sfruttano le vulnerabilità delle applicazioni di rete.

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, possono espandersi in tutto il mondo entro poche ore o persino pochi minuti dal rilascio. Questa capacità di replicarsi in modo indipendente e rapido li rende molto più pericolosi rispetto ad altri tipi di malware.

Un worm attivato in un sistema può provocare diversi inconvenienti: può eliminare file, ridurre le prestazioni del sistema e perfino disattivare programmi. La sua natura lo qualifica come "mezzo di trasporto" per altri tipi di infiltrazioni.

Se il computer è infettato da un worm, si consiglia di eliminare i file infetti poiché è probabile che contengano codice dannoso.

Tra i worm più noti si segnalano: Lovsan/Blaster, Stration/Warezov, Bagle e Netsky.

6.1.3 Trojan horse

Storicamente, i trojan horse sono stati definiti come una classe di infiltrazioni che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli a eseguirli. Tuttavia, è importante notare che ciò era vero in passato, ma oggi tali programmi non hanno più la necessità di camuffarsi. Il loro unico scopo è quello di infiltrarsi il più facilmente possibile e portare a termine i loro obiettivi dannosi. Il termine "Trojan horse" ("cavallo di Troia") ha assunto un'accezione molto generale che indica un'infiltrazione che non rientra in una classe specifica di infiltrazioni.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie:

- **Downloader**: programma dannoso in grado di scaricare altre infiltrazioni da Internet
- **Dropper**: tipo di trojan horse concepito per installare sui computer compromessi altri tipi di malware
- **Backdoor**: applicazione che comunica con gli autori degli attacchi remoti, consentendo loro di ottenere l'accesso a un sistema e assumerne il controllo
- **Keylogger** (registratore delle battute dei tasti): programma che registra ogni battuta di tasto effettuata da un utente e che invia le informazioni agli autori degli attacchi remoti
- **Dialer**: programma progettato per connettersi a numeri con tariffe telefoniche molto elevate. È quasi impossibile che un utente noti la creazione di una nuova connessione. I dialer possono causare danni solo agli utenti con connessione remota che ormai viene utilizzata sempre meno frequentemente.

Solitamente, i trojan horse assumono la forma di file eseguibili con estensione .exe. Se sul computer in uso viene rilevato un file classificato come trojan horse, si consiglia di eliminarlo, poiché probabilmente contiene codice dannoso.

Tra i trojan più noti si segnalano: NetBus, Trojandownloader. Small.ZL, Slapper.

6.1.4 Rootkit

I rootkit sono programmi dannosi che forniscono agli autori degli attacchi su Internet l'accesso illimitato a un sistema, nascondendo tuttavia la loro presenza. I rootkit, dopo aver effettuato l'accesso a un sistema (di norma, sfruttando una vulnerabilità del sistema), utilizzano le funzioni del sistema operativo per non essere rilevati dal software antivirus: nascondono i processi, i file, i dati del registro di Windows, ecc. Per tale motivo, è quasi impossibile rilevarli utilizzando le tradizionali tecniche di testing.

Per bloccare i rootkit, sono disponibili due livelli di rilevamento:

1) Quando tentano di accedere a un sistema. Non sono ancora presenti e pertanto sono inattivi. La maggior parte dei sistemi antivirus è in grado di eliminare i rootkit a questo livello (presupponendo che riescano effettivamente a rilevare tali file come infetti).

2) Quando sono nascosti dal normale testing. Gli utenti di ESET Mail Security hanno il vantaggio di poter utilizzare la tecnologia Anti-Stealth che è in grado di rilevare ed eliminare anche i rootkit attivi.

6.1.5 Adware

Adware è l'abbreviazione di software con supporto della pubblicità ("advertising-supported software"). Rientrano in questa categoria i programmi che consentono di visualizzare materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup contenente pubblicità all'interno di un browser Internet oppure ne modificano la pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono ai loro sviluppatori di coprire i costi di sviluppo delle applicazioni che, in genere, si rivelano molto utili.

L'adware non è di per sé pericoloso, anche se gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere anche funzioni di rilevamento, al pari dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un

programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware.

Alcuni programmi non verranno installati senza l'installazione dell'adware. In caso contrario, le loro funzionalità saranno limitate. Ciò significa che l'adware potrebbe accedere di frequente al sistema in modo "legale", poiché l'utente ne ha dato il consenso. In tal caso, prevenire è sempre meglio che curare. Se in un computer viene rilevato un file adware, è consigliabile eliminarlo, in quanto è molto probabile che contenga codice dannoso.

6.1.6 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso o la consapevolezza dell'utente. Gli spyware si avvalgono di funzioni di monitoraggio per inviare dati statistici di vario tipo, tra cui un elenco dei siti Web visitati, indirizzi e-mail della rubrica dell'utente o un elenco dei tasti digitati.

Gli autori di spyware affermano che lo scopo di tali tecniche è raccogliere informazioni aggiuntive sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è legato al fatto che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte verranno utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti bancari e così via. I programmi spyware sono frequentemente accoppiati a versioni gratuite di un programma creato dal relativo autore per generare profitti o per offrire un incentivo all'acquisto del software. Spesso, gli utenti sono informati della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire l'aggiornamento a una versione a pagamento che non lo contiene.

Esempi di prodotti freeware noti associati a programmi spyware sono le applicazioni client delle reti P2P (peer-to-peer). Spyfalcon o Spy Sheriff (e molti altri ancora) appartengono a una sottocategoria di spyware specifica, poiché si fanno passare per programmi antispyware ma in realtà sono essi stessi applicazioni spyware.

Se in un computer viene rilevato un file spyware, è consigliabile eliminarlo in quanto è molto probabile che contenga codice dannoso.

6.1.7 Programmi di compressione

Un programma di compressione è un eseguibile compresso autoestraente che combina vari tipi di malware in un unico pacchetto.

I programmi di compressione più comuni sono UPX, PE_Compact, PKLite e ASPack. Se compresso, lo stesso malware può essere rilevato in modo diverso, mediante l'utilizzo di un programma di compressione diverso. I programmi di compressione sono anche in grado di mutare le proprie "firme" nel tempo, rendendo più complessi il rilevamento e la rimozione dei malware.

6.1.8 Exploit Blocker

L'Exploit Blocker è progettato per rafforzare le applicazioni comunemente utilizzate, come browser Web, lettori PDF, client di posta o componenti di MS Office. Il sistema monitora il comportamento dei processi ai fini del rilevamento di attività sospette che potrebbero indicare la presenza di un exploit e aggiunge un altro livello di protezione, in grado di rilevare gli autori degli attacchi informatici con un maggior livello di precisione, utilizzando una tecnologia completamente differente rispetto alle comuni tecniche di rilevamento di file dannosi.

Nel momento in cui l'Exploit Blocker identifica un processo sospetto, lo interrompe immediatamente e registra i dati relativi alla minaccia, che vengono quindi inviati al sistema cloud di ESET Live Grid. Le informazioni vengono elaborate dal laboratorio delle minacce ESET e utilizzate ai fini di una maggiore protezione degli utenti contro minacce sconosciute e attacchi zero-day (malware di nuova concezione per i quali non sono disponibili soluzioni preconfigurate).

6.1.9 Scanner memoria avanzato

Lo Scanner memoria avanzato lavora congiuntamente all'Exploit Blocker per garantire una maggiore protezione contro malware concepiti allo scopo di eludere il rilevamento dei prodotti antimalware mediante l'utilizzo di pratiche di offuscamento e/o crittografia. Qualora i metodi di emulazione o di euristica ordinari non siano in grado di rilevare una minaccia, lo Scanner memoria avanzato identifica il comportamento sospetto ed effettua un controllo delle minacce presenti nella memoria del sistema. Questa soluzione si rivela efficace persino contro i malware che utilizzano pratiche di offuscamento ottimizzate. Diversamente dall'Exploit Blocker, lo Scanner memoria avanzato rappresenta un metodo post-esecuzione. Ciò implica un rischio di esecuzione di attività dannose prima del rilevamento di una minaccia. Tuttavia, qualora le altre tecniche di rilevamento disponibili non si rivelino efficaci, questo sistema offre un livello di protezione aggiuntivo.

6.1.10 Applicazioni potenzialmente pericolose

Esistono molti programmi legali utili per semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. ESET Mail Security offre la possibilità di rilevare tali minacce.

Applicazioni potenzialmente pericolose è la classificazione utilizzata per il software legale e commerciale. Questa classificazione include programmi quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente).

Se si rileva la presenza di un'applicazione potenzialmente pericolosa in esecuzione sul computer (che non è stata installata dall'utente) rivolgersi all'amministratore di rete o rimuovere l'applicazione.

6.1.11 Applicazioni potenzialmente indesiderate

Le **Applicazioni potenzialmente indesiderate** (PUA) non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso prima dell'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

- Nuove finestre mai visualizzate in precedenza (popup, annunci pubblicitari)
- Attivazione ed esecuzione di processi nascosti
- Maggiore utilizzo delle risorse del sistema
- Modifiche dei risultati di ricerca
- Applicazione che comunica con server remoti

6.2 E-mail

L'e-mail o electronic mail è una moderna forma di comunicazione che presenta numerosi vantaggi. È flessibile, veloce e diretta e ha svolto un ruolo cruciale nella proliferazione di Internet all'inizio degli anni novanta.

Purtroppo, a causa dell'elevato livello di anonimità, i messaggi e-mail e Internet lasciano ampio spazio ad attività illegali come lo spam. Lo spam include annunci pubblicitari non desiderati, hoax e proliferazione di software dannoso o malware. Ad aumentare ulteriormente i disagi e i pericoli è il fatto che i costi di invio dello spam sono minimi e gli autori dispongono di numerosi strumenti per acquisire nuovi indirizzi e-mail. Il volume e la varietà dello spam ne rende inoltre estremamente difficoltoso il monitoraggio. Maggiore è il periodo di utilizzo dell'indirizzo e-mail, più elevata sarà la possibilità che finisca in un database per motori di spam. Di seguito sono riportati alcuni suggerimenti per la prevenzione di messaggi e-mail indesiderati:

- Se possibile, evitare di pubblicare il proprio indirizzo e-mail su Internet
- Fornire il proprio indirizzo e-mail solo a utenti considerati attendibili
- Se possibile, non utilizzare alias comuni. Maggiore è la complessità degli alias, minore sarà la probabilità che vengano rilevati
- Non rispondere a messaggi di spam già recapitati nella posta in arrivo

- Quando si compilano moduli su Internet, prestare particolare attenzione a selezionare opzioni quali "Sì, desidero ricevere informazioni".
- Utilizzare indirizzi e-mail "specifici", ad esempio uno per l'ufficio, uno per comunicare con gli amici e così via
- Cambiare di tanto in tanto l'indirizzo e-mail
- Utilizzare una soluzione antispam

6.2.1 Pubblicità

La pubblicità su Internet è una delle forme di pubblicità in maggiore crescita. I vantaggi principali dal punto di vista del marketing sono i costi ridotti e un livello elevato di immediatezza. I messaggi vengono inoltre recapitati quasi immediatamente. Molte società utilizzano strumenti di marketing via e-mail per comunicare in modo efficace con i clienti attuali e potenziali.

Questo tipo di pubblicità è legittimo, perché si potrebbe essere interessati a ricevere informazioni commerciali su determinati prodotti. Molte società inviano tuttavia messaggi di contenuto commerciale non desiderati. In questi casi, la pubblicità tramite e-mail supera il limite e diventa spam.

La quantità di messaggi e-mail non desiderati diventa così un problema e non sembra diminuire. Gli autori di messaggi e-mail non desiderati tentano spesso di mascherare i messaggi spam come messaggi legittimi.

6.2.2 Hoax: truffe e bufale

Un hoax è un messaggio contenente informazioni non veritiere diffuso su Internet che viene in genere inviato via e-mail e tramite strumenti di comunicazione come ICQ e Skype. Il messaggio stesso è in genere una burla o una leggenda metropolitana.

Gli hoax virus tentano di generare paura, incertezza e dubbio ("Fear, Uncertainty and Doubt" - FUD) nei destinatari, inducendoli a credere che nei relativi sistemi è presente un "virus non rilevabile" in grado di eliminare file e recuperare password o di eseguire altre attività dannose.

Alcuni hoax richiedono ai destinatari di inoltrare messaggi ai loro contatti, aumentandone così la diffusione. Esistono hoax via cellulare, richieste di aiuto, offerte di denaro dall'estero e così via. Spesso è impossibile determinare l'intento dell'autore del messaggio.

È molto probabile che i messaggi che invitano a essere inoltrati a tutti i propri conoscenti siano hoax. Su Internet sono presenti molti siti Web in grado di verificare l'autenticità di un messaggio e-mail. Prima di inoltrarlo, effettuare una ricerca in Internet per qualsiasi messaggio si sospetti essere hoax.

6.2.3 Phishing

Il termine phishing definisce un'attività illegale che si avvale di tecniche di ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni confidenziali). Lo scopo è quello di ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via.

Di norma, l'accesso viene ricavato tramite l'invio di messaggi e-mail che imitano quelli di una persona o società affidabile (istituto finanziario, compagnia di assicurazioni). Il messaggio e-mail sembra autentico e presenta immagini e contenuti che possono indurre a credere che provenga effettivamente da un mittente affidabile. Tali messaggi chiedono all'utente, con vari pretesti (verifica dati, operazioni finanziarie), di immettere alcuni dati personali: numeri di conto bancario o nomi utente e password. Tali dati, se inviati, possono essere facilmente rubati e utilizzati in modo illegale.

Le banche, le compagnie di assicurazioni e altre società legittime non chiederanno mai di rivelare nomi utente e password in messaggi e-mail non desiderati.

6.2.4 Riconoscimento messaggi indesiderati di spam

Generalmente, esistono alcuni indicatori che consentono di identificare i messaggi spam (e-mail indesiderate) nella casella di posta. Un messaggio può essere considerato un messaggio spam se soddisfa almeno alcuni dei criteri riportati di seguito:

- L'indirizzo del mittente non appartiene a nessuno degli utenti presenti nell'elenco dei contatti
- Agli utenti viene offerta una grossa somma di denaro, purché si impegnino ad anticipare una piccola somma di denaro
- Viene chiesto di immettere, con vari pretesti (verifica di dati, operazioni finanziarie), alcuni dati personali, tra cui numeri di conti bancari, nomi utente, password e così via
- È scritto in una lingua straniera
- Viene chiesto di acquistare un prodotto a cui non si è interessati. Se tuttavia si decide di acquistarlo, è consigliabile verificare che il mittente del messaggio sia un id attendibile (contattare il produttore originale)
- Alcuni termini contengono errori di ortografia nel tentativo di aggirare il filtro antispam, ad esempio "vaigra" invece di "viagra" e così via

6.2.4.1 Regole

Nell'ambito delle soluzioni antispam e dei client di posta, le regole sono strumenti per manipolare le funzioni e-mail. Sono composte da due parti logiche:

1) Condizione (ad esempio, messaggio in arrivo da un determinato indirizzo)

2) Azione (ad esempio, eliminazione del messaggio, spostamento in una cartella specifica)

Il numero e la combinazione di regole varia a seconda della soluzione antispam. Queste regole rappresentano misure contro i messaggi di spam (e-mail indesiderate). Esempi tipici:

- Condizione: un messaggio e-mail in arrivo contiene alcune parole generalmente inserite nei messaggi di spam 2. Azione: eliminare il messaggio
- Condizione: un messaggio e-mail in arrivo contiene un allegato con estensione .exe 2. Azione: eliminare l'allegato e recapitare il messaggio alla casella di posta
- Condizione: un messaggio e-mail in arrivo è stato inviato dal datore di lavoro dell'utente 2. Azione: spostare il messaggio nella cartella "Lavoro"

Si consiglia di utilizzare una combinazione di regole nei programmi antispam per semplificare l'amministrazione e filtrare più efficacemente i messaggi di spam.

6.2.4.2 Filtro Bayes

Il filtraggio di spam Bayes è un tipo efficace di filtraggio e-mail, utilizzato da quasi tutti i prodotti antispam. È in grado di identificare messaggi e-mail indesiderati con un elevato livello di precisione e può essere utilizzato in base ai singoli utenti.

La funzionalità si basa sul principio seguente: il processo di riconoscimento avviene nella prima fase. L'utente contrassegna manualmente un numero sufficiente di messaggi come legittimi o come spam (in genere 200/200). Il filtro analizza entrambe le categorie e riconosce, ad esempio, che i messaggi spam contengono in genere parole come "rolex" o "viagra", mentre i messaggi legittimi sono inviati da familiari o da indirizzi presenti nell'elenco contatti dell'utente. Se viene elaborato un numero sufficiente di messaggi, il filtro Bayes è in grado di assegnare un determinato "indice di spam" a ciascun messaggio e stabilire se si tratta di spam o meno.

Il vantaggio principale offerto dal filtro Bayes è la flessibilità del metodo. Se ad esempio un utente è un biologo, verrà assegnato un indice di probabilità basso a tutti i messaggi e-mail in arrivo che riguardano la biologia o campi di studio correlati. Se un messaggio comprende parole che potrebbero identificarlo normalmente come non richiesto, ma proviene da un utente presente nell'elenco di contatti dell'utente, verrà contrassegnato come legittimo, poiché

per i mittenti contenuti in un elenco di contatti diminuisce la probabilità generale di spam.

6.2.4.3 Whitelist

In generale, una whitelist è un elenco di voci o di persone accettate a cui è stata concessa l'autorizzazione di accesso. Il termine "whitelist di posta" definisce un elenco di contatti da cui l'utente desidera ricevere messaggi. Tali whitelist sono basate su parole chiave ricercate negli indirizzi e-mail, nei nomi di domini o negli indirizzi IP.

Se una whitelist funziona in "modalità di esclusività", i messaggi provenienti da qualsiasi altro indirizzo, dominio o indirizzo IP non verranno ricevuti. Se una whitelist non è esclusiva, tali messaggi non verranno eliminati ma solo filtrati in altro modo.

Una whitelist si basa sul principio opposto di quello di una blacklist. Le whitelist sono relativamente facili da mantenere, molto di più rispetto alle blacklist. Si consiglia di utilizzare sia la whitelist che la blacklist per filtrare più efficacemente i messaggi di spam.

6.2.4.4 Blacklist

In genere, una blacklist è un elenco di persone o elementi non accettati o vietati. Nel mondo virtuale, è una tecnica che consente di accettare messaggi provenienti da tutti gli utenti non presenti in questo elenco.

Esistono due tipi di blacklist: quelle create dall'utente all'interno della propria applicazione antispam e blacklist di tipo professionale, aggiornate regolarmente e create da istituzioni specializzate che sono disponibili su Internet.

È essenziale utilizzare le blacklist per bloccare lo spam in modo efficace. Tali elenchi sono tuttavia difficili da gestire, perché ogni giorno si presentano nuovi elementi da bloccare. È pertanto consigliabile utilizzare sia whitelist che blacklist per filtrare in modo più efficace lo spam.

6.2.4.5 Controllo lato server

Il controllo lato server è una tecnica che consente di identificare spam di massa in base al numero di messaggi ricevuti e alle reazioni degli utenti. Ogni messaggio lascia un'"impronta" digitale univoca in base al suo contenuto. Il numero ID univoco non fornisce alcuna informazione in merito al contenuto del messaggio e-mail. Due messaggi identici avranno impronte identiche, mentre messaggi diversi avranno impronte diverse.

Se un messaggio viene contrassegnato come spam, l'impronta corrispondente viene inviata al server. Se il server riceve più impronte identiche (che corrispondono a un determinato messaggio di spam), l'impronta viene memorizzata nel database di impronte di spam. Durante il controllo dei messaggi in arrivo, il programma invia le impronte dei messaggi al server. Il server restituisce informazioni sulle impronte corrispondenti ai messaggi già contrassegnati dagli utenti come spam.